КОД БЕЗОПАСНОСТИ

Средство криптографической защиты информации

Континент TLS-клиент

Версия 2

Руководство по эксплуатации

RU.88338853.501430.020 91



© Компания "Код Безопасности", 2019. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

Этот документ входит в комплект поставки изделия. На него распространяются все условия лицензионного соглашения. Без специального письменного разрешения компании "Код Безопасности" этот документ или его часть в печатном или электронном виде не могут быть подвергнуты копированию и передаче третьим лицам с коммерческой целью.

Информация, содержащаяся в этом документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны компании "Код Безопасности".

Почтовый адрес:	**115127, Россия, Москва, а/я 66** **ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**http://www.securitycode.ru**

Оглавление

Введение ... **4**

Общие сведения ... **5**

Назначение и основные функции ... 5
Принципы функционирования ... 6
Сертификаты открытых ключей ... 6
Контроль целостности ... 6
Назначение ключевых носителей ... 7
Аудит ... 8

Установка, удаление, восстановление и обновление программного обеспечения ... **9**

Установка программного обеспечения TLS-клиента ... 9
Установка дополнительного ПО ... 10
Удаление ... 10
Восстановление ... 10
Обновление ПО ... 11

Настройка и эксплуатация ... **12**

Ввод в эксплуатацию ... 12
Подготовка к работе ... 12
Запуск TLS-клиента ... 12
Пользовательский интерфейс основного окна ... 13
Регистрация TLS-клиента ... 13
Управление сертификатами ... 15
Начальная настройка ... 15
Просмотр сведений о сертификате ... 16
Создание ключа и запроса на сертификат ... 16
Варианты использования криптопровайдера при формировании закрытого ключа пользователя ... 20
Импорт сертификата ... 23
Управление CRL ... 25
Настройка CDP ... 25
Загрузка CRL ... 25
Настройка соединений ... 26
Настройка параметров работы TLS-клиента ... 27
Основные настройки ... 28
Настройки прокси ... 30
Управление конфигурацией ... 32
Настройки обновления ... 32
Настройка аудита ... 34
Внешний вид ... 35
Эксплуатация TLS-клиента ... 35
Доступ к защищенным ресурсам ... 35
Контроль целостности ... 36

Приложение ... **39**

Требования к сертификатам ... 39
Структура и содержание сертификата Сервера ... 39
Структура и содержание сертификата пользователя ... 40
Список регистрируемых событий ... 40

Введение

Данное руководство предназначено для пользователей и администраторов изделия "Средство криптографической защиты информации "Континент TLS-клиент". Версия 2" (далее — TLS-клиент). В нем содержатся сведения, необходимые для установки, настройки и эксплуатации TLS-клиента.

Сайт в интернете. Информация о продуктах компании "Код Безопасности" представлена на сайте https://www.securitycode.ru/products/.

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8-495-982-30-20 или по электронной почте support@securitycode.ru. Страница службы технической поддержки на сайте компании "Код Безопасности": https://www.securitycode.ru/services/tech-support/.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании https://www.securitycode.ru/company/education/training-courses/. Связаться с представителем компании по вопросам организации обучения можно по электронной почте (education@securitycode.ru).

Глава 1
Общие сведения

Назначение и основные функции

TLS-клиент предназначен для реализации защищенного доступа удаленных пользователей к веб-ресурсам корпоративной сети по каналам связи общих сетей передачи данных.

TLS-клиент обеспечивает следующие основные функции:

- реализация TLS-аутентификации (в том числе односторонней) на основе технологии открытых ключей (используются сертификаты открытых ключей стандарта X.509 версии 3. Также TLS-клиент поддерживает работу с ключевыми носителями, изданными в "КриптоПро УЦ" 1.5);
- установление защищенного соединения с сервером на базе протокола HTTPS и обмен данными с ресурсами корпоративной сети;
- возможность работы с серверами, поддерживающими протокол TLS 1.0, 1.2;
- хранение ключевой информации в защищенном контейнере;
- проверка сертификатов ключей по списку отозванных сертификатов (CRL);
- регистрация событий, связанных с настройкой и функционированием TLS-клиента, в журнале Windows;
- контроль целостности программного обеспечения (ПО), передаваемой и хранимой информации;
- возможность автоматического обновления ПО и автоматической конфигурации перечня защищенных ресурсов;
- очистка сессионной, включая криптографическую, информации при разрыве соединения.

TLS-клиент функционирует совместно с изделиями "Средство криптографической защиты информации "Континент TLS VPN Сервер". Версия 1.2", "Средство криптографической защиты информации "Континент TLS-сервер". Версия 2" (далее — TLS-сервер).

TLS-клиент используется для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну.

TLS-клиент реализуется в двух исполнениях:

- исполнение 1 — соответствует требованиям ФСБ России к криптографическим средствам класса КС1;
- исполнение 2 — соответствует требованиям ФСБ России к криптографическим средствам класса КС2, работает совместно с сертифицированным ФСБ России аппаратно-программным модулем доверенной загрузки "Программно-аппаратный комплекс "Соболь" (далее — ПАК "Соболь").

TLS-клиент устанавливается на компьютеры, удовлетворяющие следующим системным требованиям:

Операционная система **Внимание!** Должны быть установлены все обновления системы	Windows 10 (кроме выпусков Education Edition, Home Edition и Insider Preview); Windows 8.1; Windows 7 SP1 (кроме выпусков Starter и Home Edition)
Процессор. Оперативная память	В соответствии с требованиями ОС, установленной на компьютер
Жесткий диск (свободное место)	150 МБ
Привод	Привод DVD/CD-ROM

Дополнительное ПО	Веб-браузер: • Google Chrome 48 или выше (для Windows 7, 8.1, 10); • Mozilla Firefox 46 или выше (для Windows 7, 8.1, 10); • Internet Explorer 8, 9, 10 (для Windows 7); • Internet Explorer 11 (для Windows 7, 8.1, 10); • Microsoft Edge (для Windows 10)

Принципы функционирования

TLS-клиент представляет собой устанавливаемое на компьютер пользователя ПО, функционирующее совместно с TLS-сервером.

Для подключения к защищаемым веб-ресурсам корпоративной сети удаленный пользователь должен в адресной строке веб-браузера ввести имя веб-ресурса. По указанному имени TLS-клиент посылает TLS-серверу запрос на создание защищенного соединения.

На основании принятого запроса TLS-сервер запускает процедуру аутентификации клиент–сервер. Аутентификация проводится на основе сертификатов открытых ключей.

После успешного завершения процедуры аутентификации выполняется генерация сеансового ключа, и между TLS-клиентом и TLS-сервером устанавливается защищенное соединение по протоколу TLS. Далее TLS-сервер направляет запрос TLS-клиента по указанному пользователем адресу веб-ресурса в защищаемую сеть. Полученный от веб-сервера ответ на запрос TLS-сервер возвращает TLS-клиенту в рамках защищенного соединения.

В случае невыполнения по каким-либо причинам требований, предъявляемых к аутентификации TLS-клиента и TLS-сервера, защищенное соединение не устанавливается и доступ пользователя к веб-ресурсу блокируется.

TLS-клиент также может формировать безопасный туннель на основе протокола TLS (далее — TLS-туннель) по алгоритмам ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 для обмена данными какого-либо приложения пользователя с защищаемым веб-ресурсом корпоративной сети. При этом обеспечивается криптографическая двусторонняя аутентификация отправителя и адресата, контроль целостности и шифрования данных информационного обмена.

Сертификаты открытых ключей

Для работы TLS-клиента требуются следующие сертификаты:

- сертификат издателя;

  Пояснение. Сертификат издателя — это корневой сертификат удостоверяющего центра, издавшего сертификат TLS-сервера.

- сертификат пользователя;
- сертификат TLS-сервера.

Поддерживается работа с ключами форматов PKCS#15, с сертификатами X.509v3 форматов DER и PEM.

Предусмотрена проверка сертификатов TLS-сервера по списку отозванных сертификатов. При наличии прямого доступа компьютера к удостоверяющему центру загрузка CRL по протоколу HTTP осуществляется автоматически. При отсутствии прямого доступа CRL должны загружаться пользователем посредством ПО TLS-клиента в хранилище сертификатов Windows.

Контроль целостности

Функция контроля целостности (КЦ) предназначена для слежения за неизменностью содержимого ПО TLS-клиента, производится с помощью утилиты "Контроль целостности" (УКЦ), входящей в дистрибутив TLS-клиента.

Контролируются файлы и каталоги дистрибутива или установленного ПО TLS-клиента, а также файлы ОС Windows.

В первом случае УКЦ производит КЦ эталонного ПО путем вычисления контрольных сумм (КС) файлов, содержащихся на диске из комплекта поставки TLS-клиента, и сравнения полученных значений со значениями, хранящимися в специальном файле дистрибутива TLS-клиента. Эти значения также приведены в формуляре TLS-клиента.

Во втором случае производится сравнение текущих значений КС контролируемых файлов и эталонных значений, рассчитанных в ходе установки TLS-клиента. Выполнение процедуры пересчета эталонных значений доступно пользователю с правами администратора Windows.

Список файлов TLS-клиента, подлежащих контролю, и значения КС для каждого из них хранятся в конфигурационном файле. Конфигурационный файл формируется при установке инсталляционного пакета.

КЦ установленного ПО осуществляется в начале работы TLS-клиента и в ходе регламентных проверок с периодичностью, заданной в настройках УКЦ. Настройка параметров КЦ разрешена только пользователям с правами администратора Windows (см. стр.**37**).

Если в ходе проведения КЦ в начале работы будет обнаружено нарушение целостности файлов, ошибка, TLS-клиент не будет запущен, а пользователь получит информационное сообщение о нарушении целостности.

Если в ходе проведения регламентной проверки будет обнаружено нарушение целостности и при этом приложение TLS-клиента будет активно, то:

- рабочие сессии с защищенными ресурсами будут продолжаться;
- создание новых сессий будет заблокировано;
- значок приложения в панели индикации Windows будет дополнен предупреждающим элементом;
- пользователь получит информационное сообщение о нарушении целостности с одновременным предложением восстановить целостность ПО.

В случае обнаружения нарушения целостности при неактивном ПО TLS-клиента будет сделана соответствующая запись в журнале событий.

При нарушении целостности пользователю будет показываться сообщение о необходимости ее восстановления:

- при каждом запуске TLS-клиента;
- каждой попытке установления сессии с защищенным ресурсом (если нарушение целостности обнаружено в ходе регламентного контроля целостности при наличии активных сессий с защищенными ресурсами).

События, связанные с КЦ, регистрируются в журнале событий Windows (см. стр.**40**).

Назначение ключевых носителей

Персональный ключевой носитель, выдаваемый пользователю администратором, предназначен для хранения ключевой информации.

Считанные ключ и сертификат сохраняются в памяти программы. При отсутствии секретного ключа в памяти программы при двусторонней аутентификации он запрашивается с выводом на экран соответствующего сообщения.

Пользователь может отказаться от чтения ключевого контейнера при двусторонней аутентификации. В этом случае соединение с защищаемым сервером не устанавливается.

Необходимо учесть:

- рабочих ключевых носителей одновременно может быть больше одного;
- на одном ключевом носителе могут быть записаны ключи для разных серверов.

В качестве ключевых носителей в комплексе могут использоваться аппаратные носители следующих типов:

- USB-флеш-накопители;
- USB-ключи — Рутокен, Рутокен Lite, Рутокен S (версия 2.0 и 3.0), Рутокен ЭЦП, JaCarta PKI, JaCarta ГОСТ, JaCarta PKI Flash, JaCarta ГОСТ Flash, eToken PRO (Java), Esmart USB Token, Esmart USB Token ГОСТ;
- смарт-карты — Рутокен ЭЦП, Рутокен Lite, JaCarta PKI, JaCarta ГОСТ, eToken PRO (Java), eToken PRO, Esmart, Esmart ГОСТ;
- идентификаторы DS1995, DS1996.

Примечание. Для использования аппаратных носителей требуется установка их драйверов и сопутствующего ПО (см. стр.10).

Аудит

Под аудитом подразумевается контроль состояния работоспособности TLS-клиента. Оценка функционирования ПО осуществляется посредством анализа произошедших событий, зарегистрированных в ходе аудита.

В рамках аудита используются два типа ресурсов, хранящихся локально на TLS-клиенте:

- системный журнал;
- лог-файлы (доступен их экспорт).

В системном журнале хранятся события от узлов сети, служб TLS-клиента, а также любые другие системные события, удовлетворяющие минимальным требованиям к хранению их в журнале.

Лог-файлы содержат более полную информацию Аудит этого типа ведется только при включенном расширенном логировании в настройках TLS-клиента (подробнее см. стр.34).

Глава 2
Установка, удаление, восстановление и обновление программного обеспечения

Установка программного обеспечения TLS-клиента

Пользователь, устанавливающий программное обеспечение (ПО) TLS-клиента, должен обладать правами администратора компьютера — входить в локальную группу администраторов.

Внимание! До начала инсталляции ПО TLS-клиента должны быть установлены последние обновления ОС Windows. Иначе в процессе установки TLS-клиента появится сообщение об ошибке и нсталляция будет прервана.

В процессе установки ПО инсталлятор анализирует установленные программные компоненты и при необходимости сообщает о недостающем ПО.

В ходе установки также будет установлено или обновлено ПО криптопровайдера "Код Безопасности CSP".

Внимание! В ходе установки TLS-клиента будет установлено ПО криптопровайдера "Код Безопасности CSP". Если планируется использовать TLS-клиент для совместной работы с криптопровайдером другой фирмы-производителя, установку стороннего ПО выполните перед инсталляцией TLS-клиента.
Если на компьютере установклена старая версия "Код Безопасности CSP, удалите ее перед началом установки TLS-клиента.

Для установки ПО:

1. Для установки TLS-клиента поместите установочный компакт-диск в привод DVD/CD-ROM и запустите на исполнение файл  Континент TLS-клиент.exe.
   На экране появится окно установки TLS-клиента с текстом лицензионного соглашения.

   Примечание. Если необходимо выбрать каталог установки файлов программы, отличный от выбора по умолчанию, или выбрать физический датчик случайных чисел ПАК "Соболь", нажмите кнопку "Настройки" и следуйте инструкциям, появляющимся на экране.

2. Прочтите лицензионное соглашение и, если вы принимаете его условия, поставьте отметку в поле "Я принимаю условия лицензионного соглашения", затем нажмите кнопку "Далее".

   Примечание. В случае появления окна системы безопасности Windows о подтверждении установки ПО нажмите кнопку "Да" или "Установить".

   Программа установки выполнит диагностику системы, после чего начнется установка ПО. После ее успешного завершения на экране появится сообщение о необходимости перезагрузки компьютера.

3. Нажмите кнопку "Перезагрузить" в окне сообщения.

   Начнется перезагрузка компьютера.

После установки TLS-клиента на рабочем столе Windows появится ярлык запуска графического приложения TLS-клиента, а в главном меню Windows появится раздел "Код Безопасности".

В этом разделе доступны следующие приложения:

Восстановление TLS-клиента	Восстановление ПО TLS-клиента из дистрибутива
Континент TLS-клиент	Запуск ПО TLS-клиента
Контроль целостности TLS-клиента	Контроль целостности дистрибутива и установленного на компьютере ПО TLS-клиента

Восстановление Код Безопасности	Восстановление криптопровайдера "Код Безопасности CSP" из дистрибутива

Установка дополнительного ПО

Если предполагается использовать СКЗИ "Континент TLS- клиент" с персональными ключевыми носителями, необходимо выполнить установку дополнительного ПО.

Для установки дополнительного ПО:

1. Если предполагается использовать персональные ключевые носители Рутокен, необходимо скачать их драйверы по ссылке: https://www.rutoken.ru/support/download/drivers-for-windows/ и выполнить действия в соответствии с инструкцией по установке драйверов https://www.rutoken.ru/manual/RutokenHowToUse.pdf.
2. Если предполагается использовать персональные ключевые носители JaCarta PKI, JaCarta ГОСТ или eToken PRO (Java), необходимо установить следующее ПО:

- единый клиент JaCarta (https://www.aladdin-rd.ru/support/downloads/43987/);
- набор драйверов и дополнительных утилит, обеспечивающий работу с электронными ключами eToken (https://www.aladdin-rd.ru/support/downloads/38524/ или https://www.aladdin-rd.ru/support/downloads/26037/).

Удаление

Удалить ПО TLS-клиент можно тремя способами:

- с помощью средства удаления и изменения программ "Программы и компоненты" ОС Windows;

  Примечание. При удалении TLS-клиент с помощью средств ОС Windows пользовательские настройки ПО на компьютере сохраняются и могут быть применены в дальнейшем, если на компьютер будет снова установлено TLS-клиент.

- утилиты восстановления ПО TLS-клиент;
- MSI-пакета, находящегося на установочном диске.

  Примечание. При удалении TLS-клиент с помощью утилиты восстановления или MSI-пакета доступна опция удаления пользовательских настроек ПО.

TLS- клиент и "Код Безопасности CSP" удаляются по отдельности в любом порядке.

Восстановление

Для восстановления ПО:

1. В главном меню ОС Windows в списке установленных программ найдите раздел "Код Безопасности" и активируйте приложение восстановления соответствующего ПО.

   На экране появится окно установки ПО.
2. Нажмите кнопку "Далее".

   На экране появится окно для восстановления или удаления ПО.
3. Выберите вариант "Восстановить", нажмите кнопку "Далее".

   На экране появится итоговое окно.
4. Нажмите кнопку "Восстановить".

   Начнется соответствующая операция, после завершения которой на экране появится окно об успешном завершении процесса.
5. Нажмите кнопку "Готово".

   На экране появится сообщение о необходимости перезагрузки системы.

6. Нажмите кнопку "Перезагрузить".

Обновление ПО

Обновить установленное ПО TLS-клиента возможно как в автоматическом, так и в ручном режиме. О настройках получения и установки обновлений см. стр.32.

Внимание! При совместной работе с СКЗИ "Континент TLS VPN Сервер". Версия 1.2" обновление посредством ПО TLS-клиента невозможно. В этом случае необходимо получить файл обновления от поставщика или с сервера обновлений ПО и установить его принудительно.

Для получения обновления ПО TLS-клиента:

1. Если в настройках TLS-клиента установлено автоматическое обновление ПО, при добавлении на TLS-сервер новых файлов обновлений на экране TLS-клиента появится информационное окно о наличии обновления. Перейдите к п.**4**.

   Внимание! Для управления обновлением ПО требуется запустить TLS-клиент от имени администратора.

2. Выберите в меню настроек TLS-клиента пункт "Обновления".

   В области отображения информации основного окна откроется соответствующее подменю.

3. Введите адрес сервера обновлений ПО в соответствующее поле.

4. Нажмите кнопку "Проверить" в области принудительного обновления ПО.

   Если адрес сервера обновления не будет задан, на экране появится сообщение о необходимости ввести его.

   На экране появится информационное окно о наличии обновления.

5. Нажмите на это окно.

   Файлы обновлений будут загружены, и на экране появится информационное сообщение:

6. Нажмите на сообщение.

   Будет произведена установка обновления, после чего на экране появится окно с требованием перезагрузки ОС.

7. Нажмите кнопку "Да".

   Будет выполнена перезагрузка ОС Windows.

Глава 3
Настройка и эксплуатация

Ввод в эксплуатацию

Подготовка к работе

Ввод TLS-клиента в эксплуатацию состоит из следующих последовательных этапов:

1. Установка TLS-клиента (см. стр.**9**).
2. Регистрация ПО (см. стр.**13**).
3. Получение сертификатов безопасности (см. стр.**15**).

   Примечание. Алгоритмы формирования электронной подписи в используемых сертификатах должны совпадать (ГОСТ Р 34.10—2001 или ГОСТ Р 34.10—2012).
4. Установка корневых и пользовательских сертификатов (см. стр.**23**).
5. Установка CRL (если необходима проверка сертификатов по CRL, см. стр.**30**).
6. Установка серверных сертификатов (если необходима соответствующая проверка, см. стр.**24**).
7. Настройка параметров работы TLS-клиента (см. стр.**27**).

   Примечание. В случае использования прокси-сервера для доступа к интернет необходимо осуществить дополнительную настройку параметров работы TLS-клиента (см. стр.**27**).
8. Настройка списка ресурсов (см. стр.**26**).

   Примечание. Для использования сетевых имен сервера или веб-ресурсов необходимо осуществить соответствующую настройку DNS-сервера или файла hosts. После внесения изменений в файл hosts необходимо перезапустить приложение TLS-клиента.

Запуск TLS-клиента

Для запуска TLS-клиента:

- Нажмите кнопку "Пуск" и выберите в главном меню Windows пункт "Код Безопасности|Континент TLS-клиент".

  Внимание! Если перед первым запуском TLS-клиента выбран "Код Безопасности CSP" а, в случае выбора биологического ДСЧ будет осуществлен набор энтропии. На экране появится окно с инструкцией. Следуйте ее указаниям и дождитесь завершения процесса накопления энтропии.

  На экране появится основное окно программы, а в правом углу панели задач ОС Windows появится значок программы.



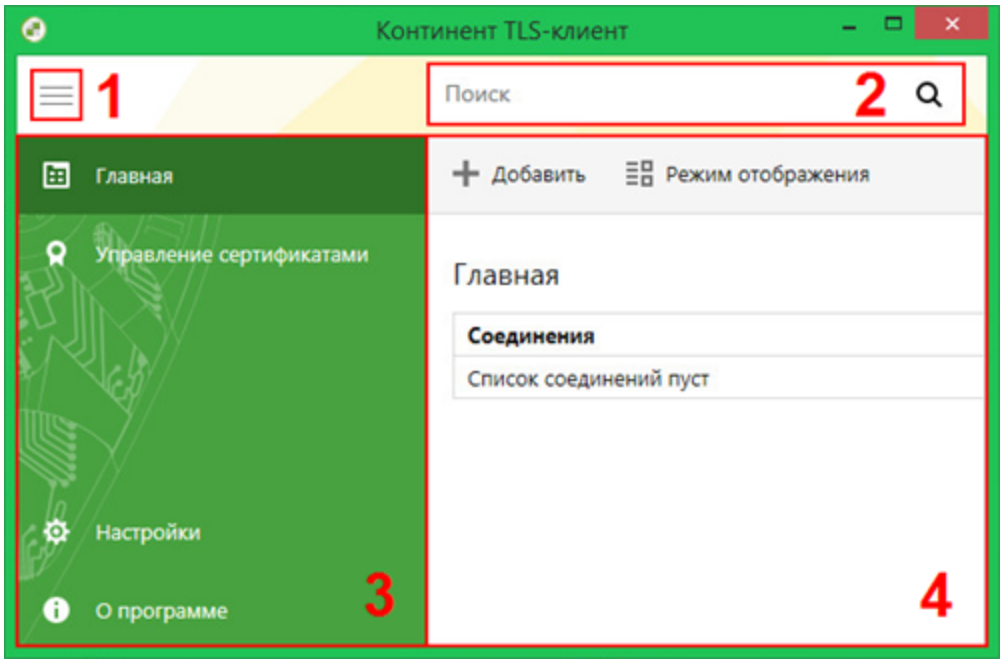
Вызов контекстного меню TLS-клиента с панели задач ОС Windows позволяет выполнить следующие команды:

- Развернуть основное окно TLS-клиента или свернуть его в системный трей.
- Сбросить текущие соединения.
- Завершить работу ПО.

При двойном нажатии на значок программы TLS-клиента левой кнопкой мыши осуществляется раскрытие или скрытие основного окна.

Примечание. Также для свертывания основного окна TLS-клиента можно использовать кнопки и в правом верхнем углу окна. Для закрытия программы выберите в контекстном меню пункт "Выход".

Пользовательский интерфейс основного окна

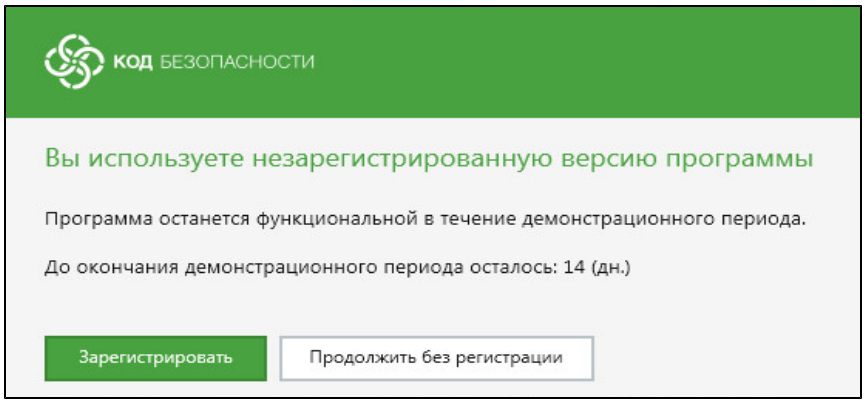


В верхней части основного окна расположена кнопка (1) переключения полного/ сжатого вида главного меню и строка (2) контекстного поиска.

В левой части основного окна расположен список разделов главного меню (3), а в правой — область отображения информации (4) активного раздела меню с панелью инструментов в верхней части.

Регистрация TLS-клиента

При первом запуске TLS- клиента пользователю будет предложено зарегистрировать программу на сервере регистрации компании "Код Безопасности". Доступна онлайн- и офлайн-регистрация.

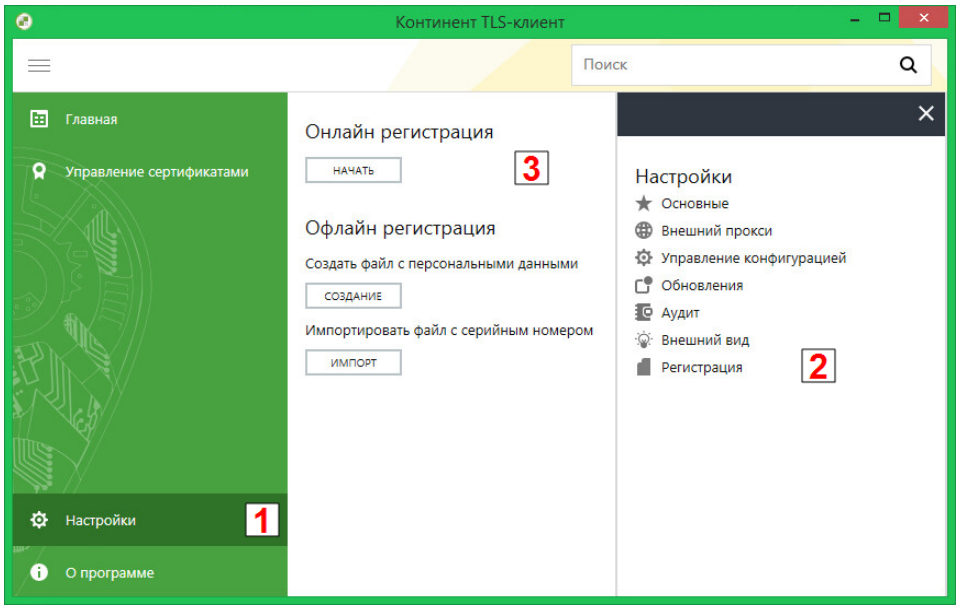


Срок работы без регистрации TLS-клиента ограничен и составляет 14 дней. Количество дней, оставшихся до окончания регистрации, отображается в разделе "О программе". Если в течение этого срока TLS-клиент не зарегистрировать, то при каждом следующем запуске он будет предлагать зарегистрироваться в системе и, в случае отказа, прекращать свою работу.

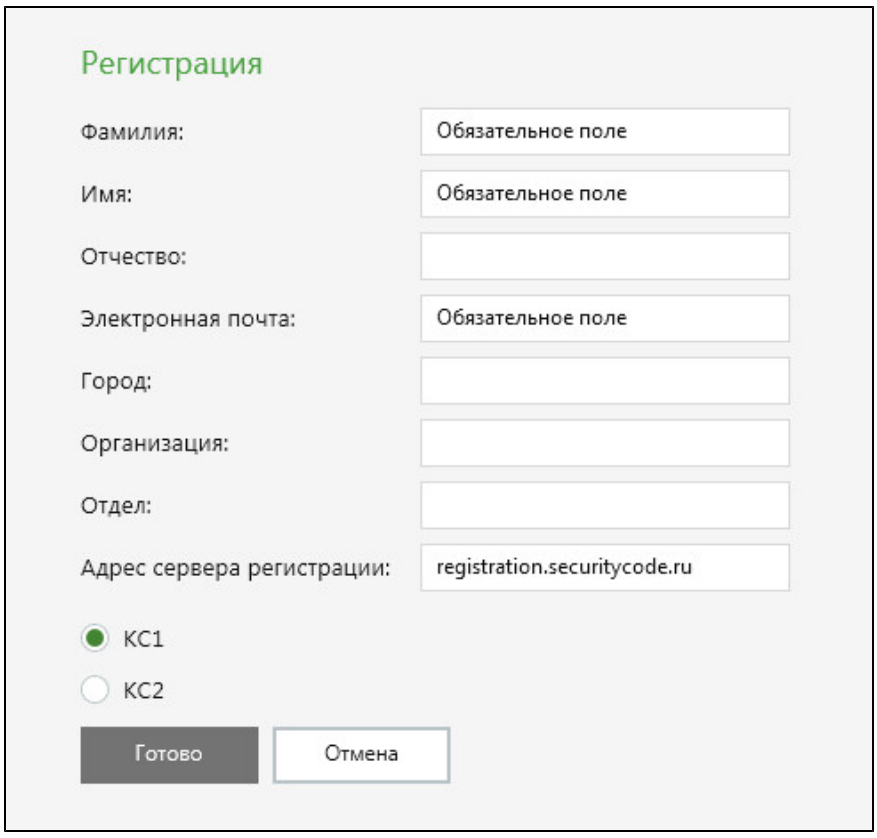
Совет. Для прекращения отображения пользователю окна регистрации при последующих запусках TLS-клиента необходимо поставить отметку в поле "Больше не спрашивать". Но рекомендуется провести процедуру регистрации при первичном запуске ПО.

Для онлайн-регистрации TLS-клиента:

1. Нажмите кнопку "Да" в окне регистрации. В случае отмены автоматического отображения окна регистрации при запуске TLS-клиента выберите в меню настроек TLS-клиента пункт "Регистрация" и нажмите кнопку "Начать".



На экране появится диалоговое окно регистрации.



2. Введите требуемые параметры и нажмите кнопку "Готово".

   Начнется процесс регистрации и подключения к указанному серверу. При его успешном завершении на экране появится соответствующее информационное окно.

После успешной отправки заполненной формы регистрации появится сообщение «Запрос на регистрацию отправлен, ждите ответа», но сам процесс будет

еще не завершен. Чтобы закончить регистрацию, через несколько дней, но не позднее 14 дней с момента установки TLS-клиента, отправьте те же данные повторно. Необходимо, чтобы данные были полностью идентичны, иначе регистрация не завершится и будет отправлена новая заявка.

После регистрацииTLS- клиента в разделе "О программе" вместо текста "Программа не зарегистрирована" появится регистрационный номер программы.

Примечание. Рекомендуется использовать офлайн-регистрацию.

Для офлайн-регистрации TLS-клиента:

1. В случае недоступности сервера регистрации выберите в меню настроек TLS-клиента пункт "Регистрация" и нажмите кнопку "Создание".

   На экране появится диалоговое окно регистрации.
2. Заполните требуемые параметры и нажмите кнопку "Готово".

   На экране появится стандартное окно сохранения файла.
3. Сохраните файл с персональными данными и передайте его на сервер регистрации для получения файла с серийным номером.
4. После получения файла с серийным номером нажмите кнопку "Импорт" в окне регистрации TLS-клиента.

   На экране появится стандартное окно выбора файла.
5. Укажите нужный файл и нажмите кнопку "Открыть".

   При успешном завершении процесса регистрации на экране появится соответствующее информационное окно.

Управление сертификатами

TLS- клиент позволяет устанавливать сертификаты в хранилище, создать криптографические контейнеры, запросы на издание сертификата пользователя и осуществлять запись их на съемный носитель или в реестр.

Начальная настройка

Для работы с TLS-клиентом необходимы корневые сертификаты, сертификаты пользователя и сертификаты сервера, получаемые в соответствии с общим порядком, установленным конкретным удостоверяющим центром. Процедура создания запроса на выдачу сертификата по алгоритму ГОСТ Р 34.10-2012 приводится на стр.**16**.

Примечание. Допустимо использовать любой действительный уникальный сертификат пользователя, выпущенный ранее удостоверяющим центром.

Для передачи сертификатов рекомендуется использовать отчуждаемый носитель.

Примечание. В качестве ключевых носителей в комплексе могут использоваться аппаратные носители следующих типов:

- USB-флеш-накопители;
- USB-ключи — Рутокен, Рутокен Lite, Рутокен S (версия 2.0 и 3.0), Рутокен ЭЦП, JaCarta PKI, JaCarta ГОСТ, JaCarta PKI Flash, JaCarta ГОСТ Flash, eToken PRO (Java), Esmart USB Token, Esmart USB Token ГОСТ;
- смарт-карты — Рутокен ЭЦП, Рутокен Lite, JaCarta PKI, JaCarta ГОСТ, eToken PRO (Java), eToken PRO, Esmart, Esmart ГОСТ;
- идентификаторы DS1995, DS1996.

После получения всех сертификатов пользователь TLS- клиента должен установить сертификаты в хранилище текущего пользователя средствами ПО TLS-клиента (см. стр. **23**), ОС Windows (см. https://technet.microsoft.com/ru-ru/library/cc754841(v=ws.11).aspx#_BKMK_addlocal) или средствами стороннего криптопровайдера:

Сертификаты	Используемый криптопровайдер	
	Код Безопасности CSP	**Сторонний**
Корневые	Средствами Windows или TLS-клиента	Средствами Windows
Пользовательские	Средствами TLS-клиента	Средствами криптопровайдера
Серверные, CRL	Средствами TLS-клиента	Средствами TLS-клиента

Просмотр сведений о сертификате

Для просмотра сертификата:

1. Выберите в главном меню TLS-клиента пункт "Управление сертификатами", а затем требуемый тип сертификатов на панели инструментов.

   В области отображения информации появится список установленных сертификатов.

2. Вызовите окно сведений о сертификате, выполнив двойной щелчок левой кнопки мыши по соответствующей строке списка установленных сертификатов.

   Откроется стандартное окно сведений о сертификате.

Примечание. Экспорт сертификата можно произвести средствами ОС Windows, для этого необходимо перейти в окне сведений о сертификате на вкладку "Состав" и нажать кнопку "Копировать в файл...".

Создание ключа и запроса на сертификат

Для создания запроса:

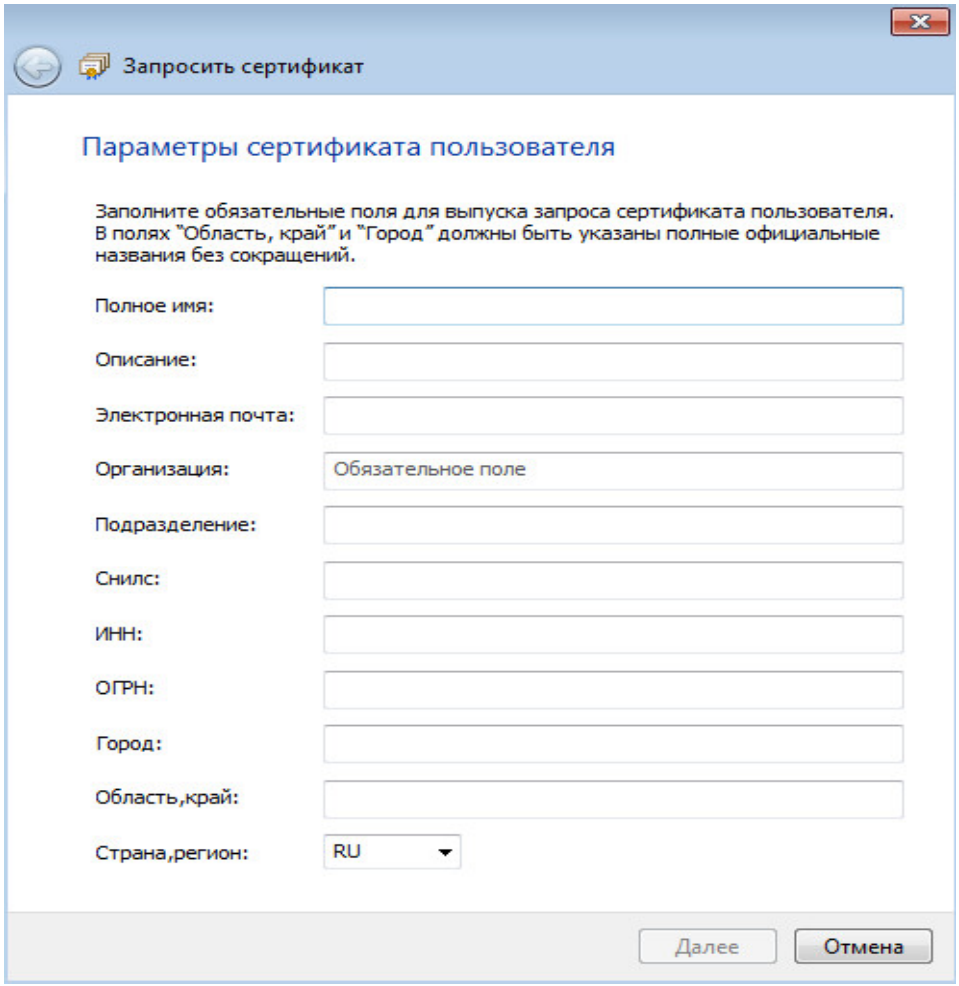
1. Выберите в главном меню TLS-клиента пункт "Управление сертификатами".

   В области отображения информации появится список установленных сертификатов.

Примечание. Для просмотра списка установленных сертификатов нажмите кнопку "Открыть хранилище" на панели инструментов.

2. На панели инструментов выберите вкладку пользовательских сертификатов и нажмите кнопку "Создать запрос".

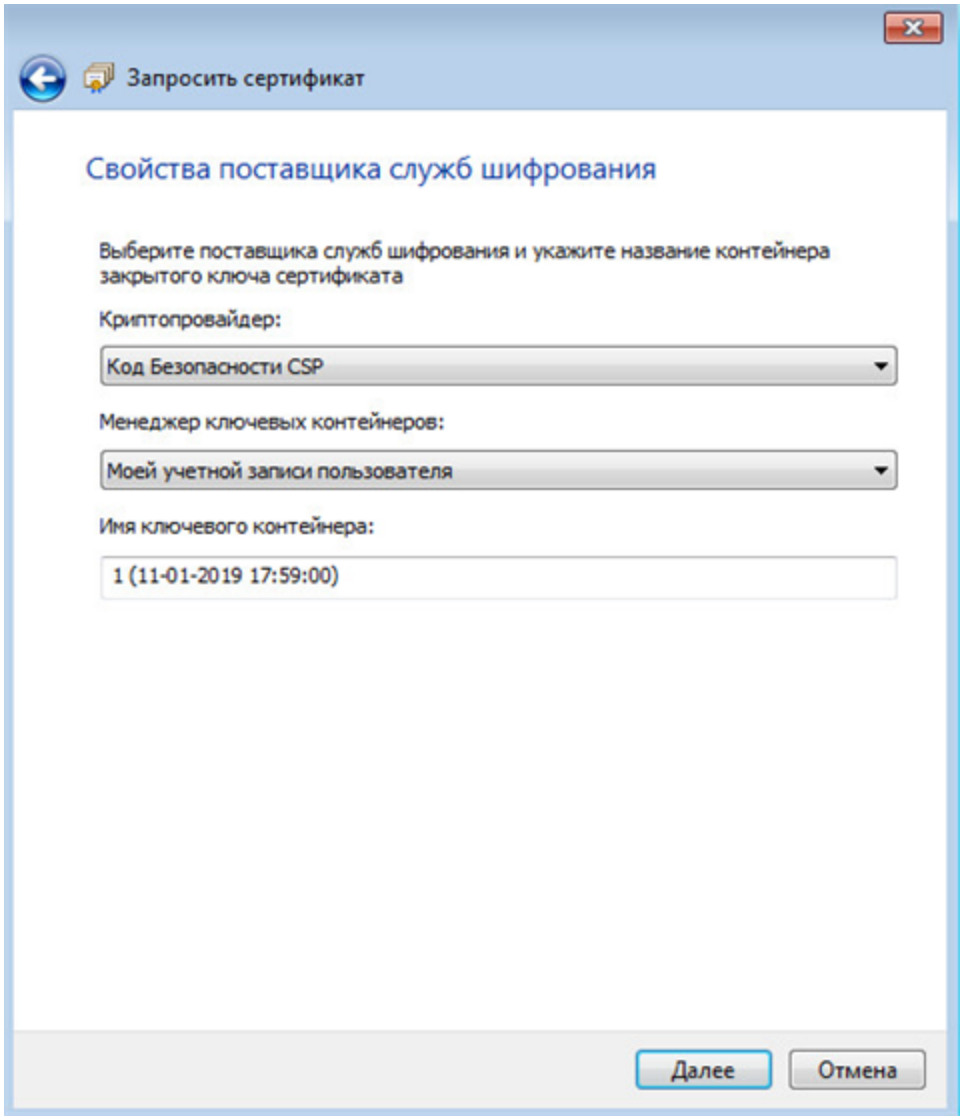
   На экране появится диалог для ввода параметров запроса.



3. Заполните параметры запроса и нажмите кнопку "Далее".

Примечание. В поле "Страна, регион" выберите из раскрывающегося списка нужное значение. К примеру, для России — RU.

На экране появится диалог выбора криптопровайдера и названия контейнера закрытого ключа сертификата.

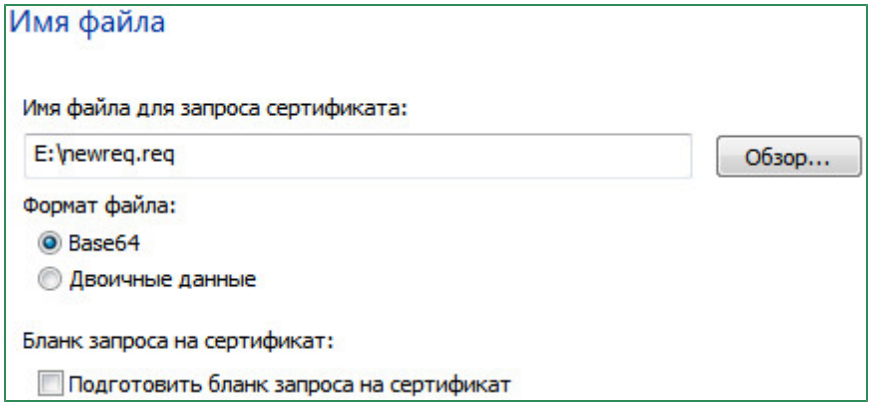


4. Заполните пункты меню:
   - в поле "Криптопровайдер" выберите в раскрывающемся списке нужное значение;
   - в поле "Менеджер ключевых контейнеров" выберите в раскрывающемся списке хранилище ключевого контейнера, в котором будет сохранен закрытый ключ сертификата пользователя;
   - в поле "Имя ключевого контейнера" измените имя ключевого контейнера, если необходимо;

   Примечание. Автоматически созданное имя контейнера по умолчанию содержит текущие время и дату.

5. Нажмите кнопку "Далее".

   На экране появится диалог для ввода имен ключевого контейнера и файла для запроса сертификата



6. Заполните пункты меню:
   - укажите имя файла для запроса сертификата;

     Примечание. По умолчанию запрос сохраняется в файле с расширением *.req и именем, содержащим имя текущего пользователя ОС Windows.

   - установите отметку в поле "Подготовить бланк запроса на сертификат", если необходимо сохранить версию запроса для печати и нажмите кнопку "Далее".

     Примечание. По умолчанию запрос сохраняется в файле с расширением *.html и именем, содержащим имя текущего пользователя ОС Windows, а также текущие время и дату.

   Для изменения расположения или имени файла с электронной или бумажной формой запроса нажмите кнопку "Обзор...", расположенную справа от соответствующего поля. В стандартном окне ОС Windows, появившемся на экране, выполните следующие действия:
   - укажите диск (папку) для создания файла;
   - укажите имя файла запроса;
   - нажмите кнопку "Сохранить".
7. Нажмите кнопку "Далее".

   Появится сообщение о завершении работы мастера запроса сертификата.
8. Проверьте корректность введенных параметров и нажмите кнопку "Готово".

   Криптопровайдер приступит к созданию закрытого ключа. Выполните следующие операции:
   - сформируйте закрытый ключ с помощью датчика случайных чисел;
   - выберите тип ключевого носителя для записи закрытого ключа;
   - введите пароль для ограничения доступа к ключевому контейнеру.

   Примечание. При наличии отметки в поле "Запомнить пароль" введенный пароль сохраняется в реестре компьютера. В дальнейшем при обращении к этому ключевому контейнеру запрос пароля на экран не выводится.

   Порядок выполнения операций зависит от используемого криптопровайдера, датчика случайных чисел и ключевого носителя, выбранного для хранения ключевой информации. Следуйте указаниям, появляющимся на экране.

   Более подробно о создании закрытого ключа см. стр.**20**.

   После завершения процедуры на экране появится сообщение о завершении создания запроса на сертификат.
9. Нажмите кнопку "ОК" в окне сообщения для завершения процедуры создания запроса.

   Внимание! Если в качестве ключевого носителя был выбран системный реестр, после создания ключевой информации не рекомендуется выполнять действия, затрагивающие системное ПО данного компьютера.

Передайте созданный файл запроса администратору безопасности. При этом можно пользоваться общедоступной сетью передачи данных, например, переслать файл как вложение электронной почты.

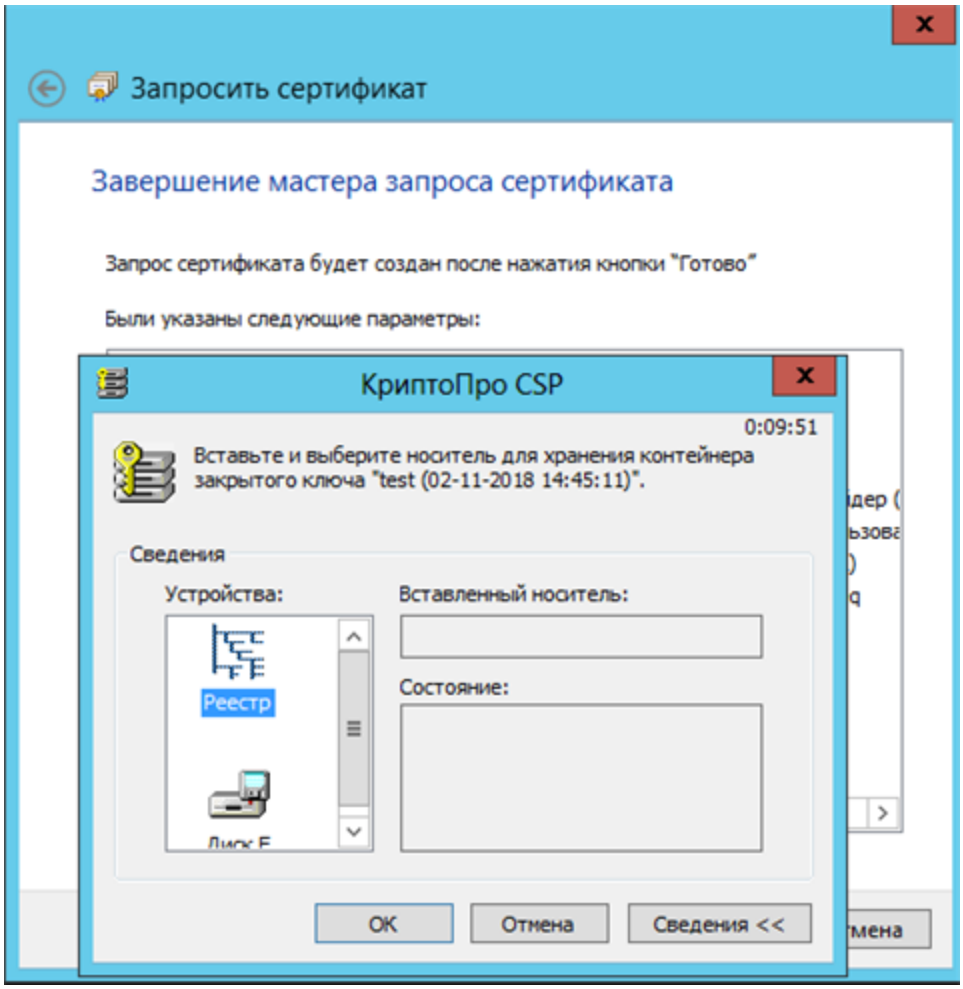
Варианты использования криптопровайдера при формировании закрытого ключа пользователя

Ниже приведены процедуры формирования закрытого ключа пользователя при создании запроса на получение сертификатов (см. стр.16). Представлены варианты использования криптопровайдеров "КриптоПро CSP" и "Код Безопасности CSP".

КриптоПро CSP

Для формирования закрытого ключа:

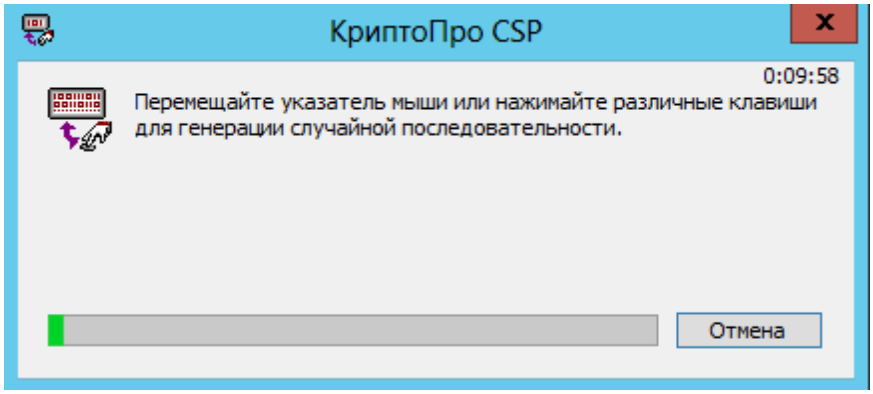
1. После нажатия в окне завершения работы мастера запроса сертификата кнопки "Готово" на экране появится окно с указанием вставить чистый ключевой носитель.



2. Вставьте носитель, нажмите кнопку "Сведения"и укажите устройство.
3. Нажмите кнопку "ОК".

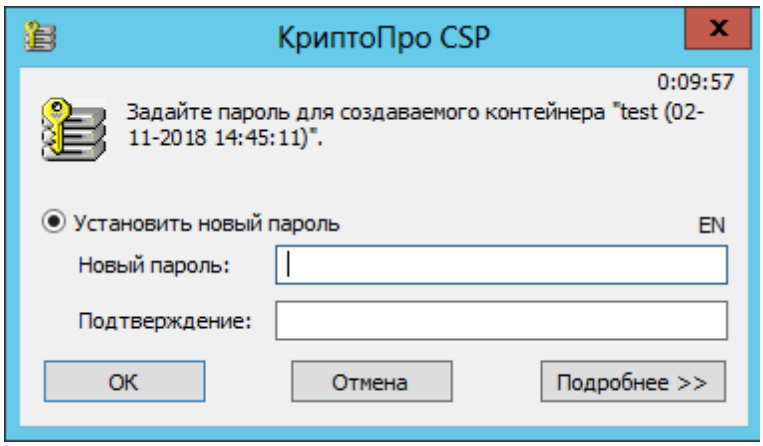
   На экране появится окно "Биологический датчик случайных чисел".

Примечание. Если в "КриптоПро CSP" настроен датчик случайных чисел ПАК "Соболь", на экране появится окно задания пароля для доступа к содержимому ключевого контейнера (см. п.**4**). Перейдите к выполнению п.**5**.



4. Следуйте инструкции на экране и дождитесь завершения создания ключа.

   На экране появится окно задания пароля для доступа к содержимому ключевого контейнера.



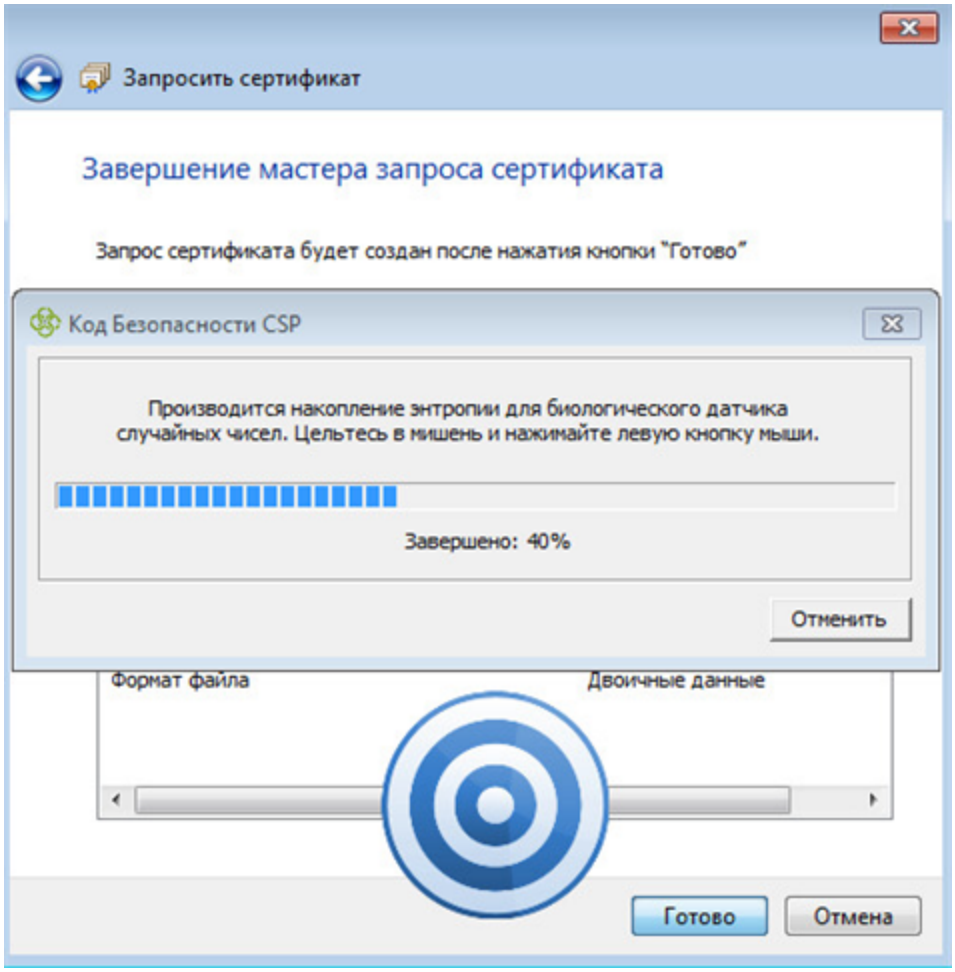
5. Введите и подтвердите пароль на создаваемый ключевой контейнер и нажмите кнопку "OK".

   Начнется запись закрытого ключа пользователя на ключевой носитель, и после ее окончания на экране появится сообщение об успешном завершении создания запроса.

Код Безопасности CSP

Для формирования закрытого ключа:

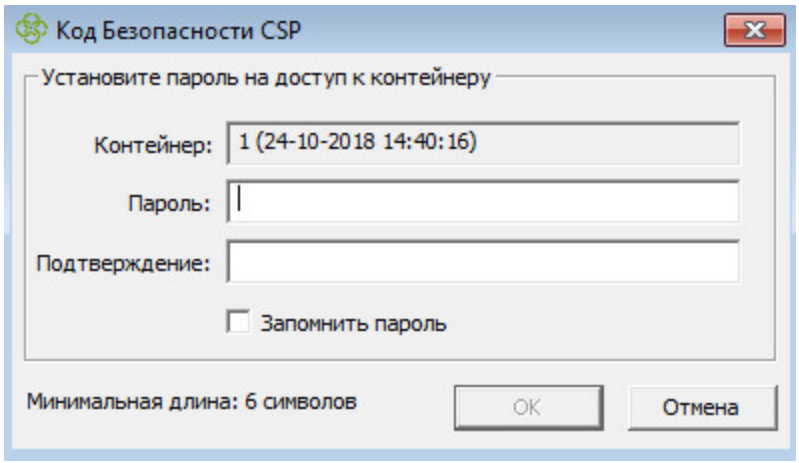
1. После нажатия в окне завершения работы мастера запроса сертификата кнопки "Готово" на экране появится окно накопления энтропии для биологического датчика случайных чисел.



Примечание. Если используется физический датчик случайных чисел ПАК "Соболь", набор энтропии выполняется автоматически и на экране не отображается. Вместо окна накопления энтропии появится окно задания пароля. Перейдите к п. **3**.

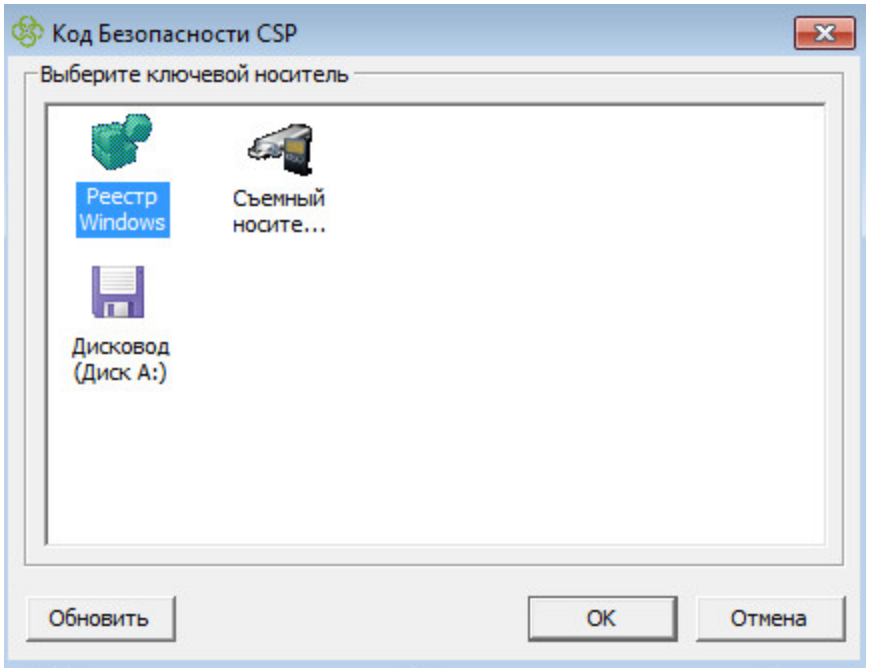
2. Следуйте указаниям инструкции на экране и дождитесь завершения набора энтропии.

   После завершения процедуры на экране появится диалог задания пароля для доступа к содержимому ключевого контейнера.



3. Введите и подтвердите пароль для доступа к создаваемому ключевому контейнеру и нажмите кнопку "ОК".

   На экране появится окно выбора ключевого носителя.



4. Выберите нужный ключевой носитель и нажмите кнопку "ОК".

Внимание! Если используемый съемный носитель содержит файлы, имена которых совпадают с именами записываемых файлов, то:

- файлы на USB-флеш-накопителе будут автоматически переименованы и сохранены;
- файлы на Рутокен будут перезаписаны с выводом запроса на выполнение операции.

Начнется создание запроса и криптографического контейнера. После успешного завершения операции на экране появится соответствующее информационное сообщение.

5. Нажмите кнопку "ОК" и извлеките носитель.

Примечание. В случае пересылки содержимого файла запроса посредством веб-интерфейса стороннего криптопровайдера откройте файл запроса в любом текстовом редакторе.

Импорт сертификата

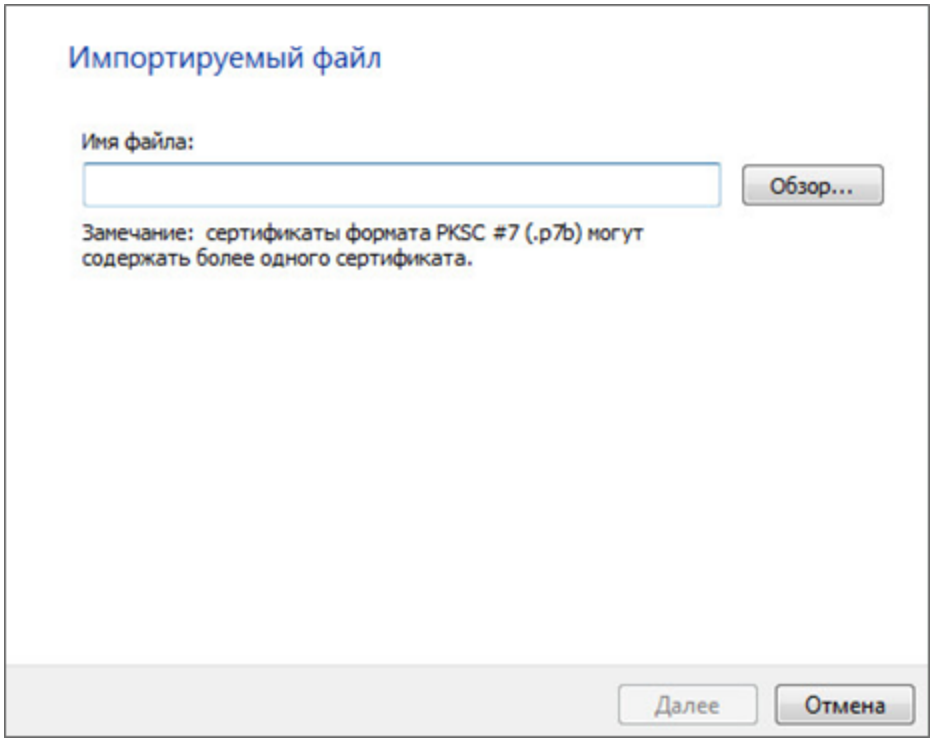
Для импорта корневого или пользовательского сертификата:

1. Выберите в главном меню TLS-клиента пункт "Управление сертификатами".

   В области отображения информации появится список установленных сертификатов.

2. На панели инструментов выберите пользовательский тип сертификатов и нажмите кнопку "Импортировать".

   На экране появится диалог настройки параметров импорта.



Примечание. При использовании "КриптоПро CSP" на экране после нажатия кнопки "Импортировать" появится сообщение о необходимости воспользоваться сторонним криптопровайдером.

3. В поле "Имя файла" укажите полный путь и имя файла с расширением .cer или .p7b, содержащего нужный сертификат, и нажмите кнопку "Далее".

   При импорте пользовательского сертификата появится окно запроса контейнера закрытого ключа сертификата. Выберите требуемый контейнер и нажмите кнопку "Далее".

   На экране появится завершающий диалог мастера установки сертификата.

4. Проверьте корректность введенных параметров импорта и нажмите кнопку "Готово".

   При импорте пользовательского сертификата появится окно запроса пароля к контейнеру закрытого ключа сертификата. Введите требуемый пароль и нажмите кнопку "ОК".

   Начнется загрузка и установка сертификата в указанное хранилище. После успешного завершения операции на экране появится соответствующее информационное сообщение.

5. Нажмите кнопку "ОК".

Для импорта серверного сертификата:

1. Выберите в главном меню TLS-клиента пункт "Управление сертификатами".

   В области отображения информации появится список установленных сертификатов.

2. На панели инструментов выберите нужную категорию и нажмите кнопку "Импортировать".

   На экране появится стандартное окно открытия файла.

3. Укажите файл загружаемого сертификата и нажмите кнопку "Открыть".

   Начнется загрузка и установка сертификата. После успешного завершения операции на экране появится соответствующее информационное сообщение.

4. Нажмите кнопку "ОК".

Управление CRL

Континент TLS-клиент позволяет в автоматическом или ручном режиме получать CDP, при этом автоматически скачивая CRL для проверки валидности используемых сертификатов. Также CRL возможно импортировать вручную.

Настройка CDP

Если же импортированные сертификаты не содержат CDP, то добавьте список CDP вручную.

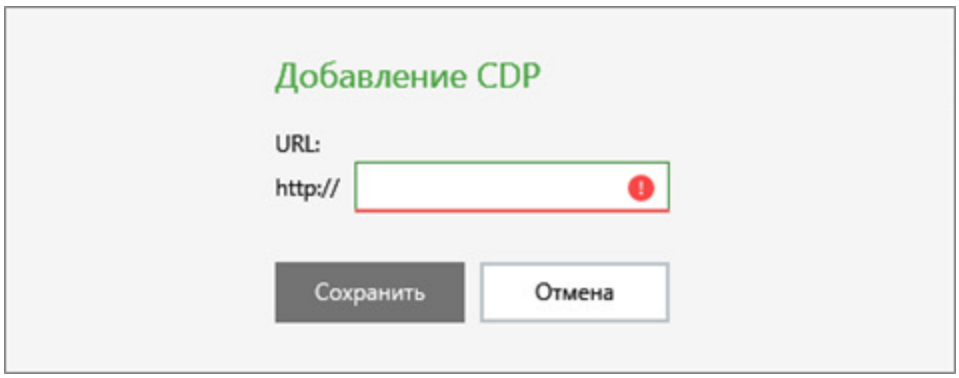
Для настройки списка CDP вручную:

1. Выберите в меню настроек СКЗИ "Континент TLS- клиент" пункт "Сертификаты", вкладку "CDP".

   В области отображения информации основного окна появится список используемых CDP.

2. Нажмите кнопку "Добавить".

   На экране появится окно для ввода URL CDP.



3. Введите адрес CDP и нажмите кнопку "Сохранить".

   На экране произойдет возврат во вкладку "CDP" с обновленным списком параметров.

4. Для редактирования или удаления добавленного пользователем CDP выберите его в соответствующем списке и нажмите на панели инструментов кнопку "Редактировать" или "Удалить".

Загрузка CRL

Автоматическая загрузка CRL происходит следующими способами:

- в результате добавления CDP после импорта сертификатов;
- согласно расписанию, заданному в настройках ПО (см. стр.27).

CRL может быть добавлен вручную следующими способами:

- импорт файла CRL;
- загрузка CRL из CDP (если он получен);
- импорт файла CRL помощью средств ОС Windows.

Если по какой-либо причине CRL не удалось скачать или он был удален из системы, то в таблице CDP отобразится состояние CRL.

Чтобы обновить сразу весь список CRL, выполните скачивание CRL вручную.

Для импорта файла CRL:

1. Выберите в главном меню СКЗИ "Континент TLS- клиент" раздел "Сертификаты" и вкладку" CDP".

   В области отображения информации появится список имеющихся CDP.

2. Нажмите кнопку "Импортировать CRL ".

   На экране появится стандартное окно открытия файла.

3. Укажите загружаемый файл CRL и нажмите кнопку "Открыть".

   Начнется загрузка. После успешного завершения операции на экране появится соответствующее информационное сообщение.

4. Нажмите кнопку "ОК".

Для загрузки файла CRL вручную:

1. Выберите в меню настроек СКЗИ "Континент TLS-клиент" пункт "Управление сертификатами", а затем вкладку "CDP" на панели инструментов.

   В области отображения информации основного окна появится список CDP.

2. Если CDP не прописан в установленном сертификате или не добавлен пользователем, то необходимо добавить CDP (см. выше, процедура настройки списка CDP).

3. Нажмите на панели инструментов кнопку "Скачать CRL".

   Начнется загрузка. После успешного завершения операции на экране появится соответствующее информационное сообщение.

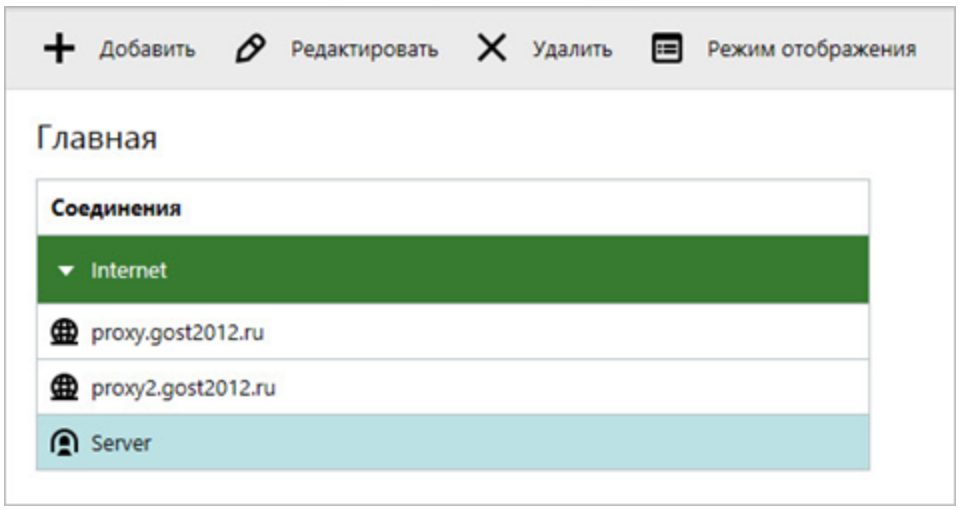
4. Нажмите кнопку "ОК".

Настройка соединений

В случае совместного использования с СКЗИ "Континент TLS-сервер". Версия 1.2" необходимо создать и настроить соединение с ним и добавить доступные ресурсы (см. ниже).

В случае совместного использования с СКЗИ "Континент TLS- сервер". Версия 2" необходимо создать настроить соединение с ним (см. ниже), получить или обновить список его ресурсов (см. стр.**27**).

С помощью панели инструментов раздела пользовать может отредактировать или удалить ранее созданное соединение, а также выбрать вид отображения информации: список или таблица.



TLS-клиент осуществляет три типа соединений:

Тип	Обозначение	Класс
TLS-сервер	▸	Сервер
HTTPS-прокси		Ресурс
Туннель		Ресурс

Для добавления нового соединения:

1. В основном меню TLS-клиента выберите пункт "Главная".

   В области отображения информации откроется список имеющихся защищенных ресурсов и TLS-серверов (соединений).

2. Выберите закладку "+ Добавить" на панели инструментов, а затем нужный класс в раскрывшемся списке.

   В правой части области отображения информации основного окна появится соответствующий список настроек.

3. Введите необходимые параметры для настройки соединения и нажмите кнопку "Сохранить".

   Внимание! Адреса серверов и ресурсов не могут быть заданы символами кириллицы.

4. Если необходимо добавить еще одно соединение, повторите пп. **2-3**.

Для редактирования соединения:

1. Для внесения изменений в параметры соединения выберите его в списке соединений и нажмите кнопку "Редактировать" на панели инструментов.

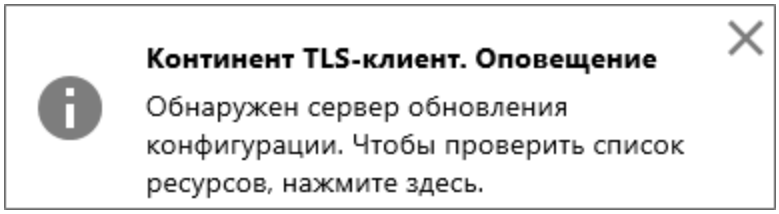
   В правой части области отображения информации основного окна появится список настроек соответствующего соединения.

2. Внесите необходимые изменения в параметры соединения и нажмите кнопку "Сохранить".

Для удаления соединения:

1. Для удаления соединения выберите его в списке соединений и нажмите кнопку "✕ Удалить" на панели инструментов.
2. Нажмите кнопку "Да" в появившемся окне подтверждения.

По умолчанию в настройках TLS- клиента установлено автоматическое обновление списка ресурсов сервера соединений (подробнее о настройках обновления ресурсов сервера см. стр.**32**). Если в результате проверки список ресурсов сервера будет признан неактуальным, рядом с адресом сервера в списке соединений появится статус "список ресурсов неактуален". На экране появится информационное сообщение о наличии обновлений. Такое же сообщение появится при добавлении нового сервера в список соединений.



Для получения или обновления списка ресурсов сервера:

1. Нажмите на информационное сообщение в правом нижнем углу экрана.

   Внимание! Если необходимо отменить обновление, нажмите ✕.

   На экране появится окно выбора сертификата.

2. Выберите требуемый сертификат и нажмите кнопку "ОК".

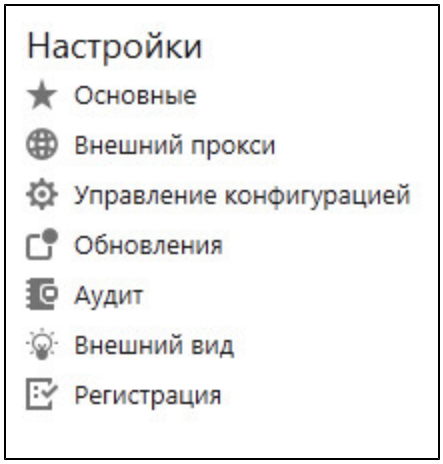
   На экране появится окно для ввода пароля для доступа к криптографическому контейнеру, если при создании контейнера не была выбрана опция "запомнить пароль".

3. Введите пароль и нажмите кнопку "ОК".

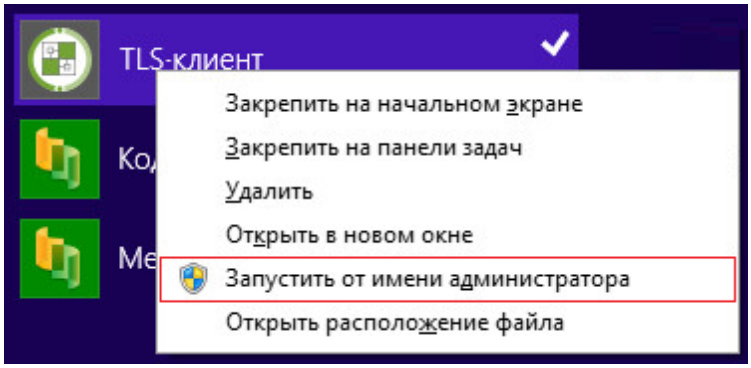
   После удачного обновления на экране появится сообщение о том, что список ресурсов сервера обновлен. Посмотреть его можно, выбрав нужный сервер в списке соединений.

Настройка параметров работы TLS-клиента

Изменение параметров ПО TLS- клиента осуществляется через меню настроек, вызов которого происходит при выборе пункта "Настройки" в главном меню основного окна TLS-клиента.



Внимание! Для изменения настроек проксирования, обновлений и туннелируемых приложений TLS-сервер следует запускать от имени администратора (через контекстное меню).

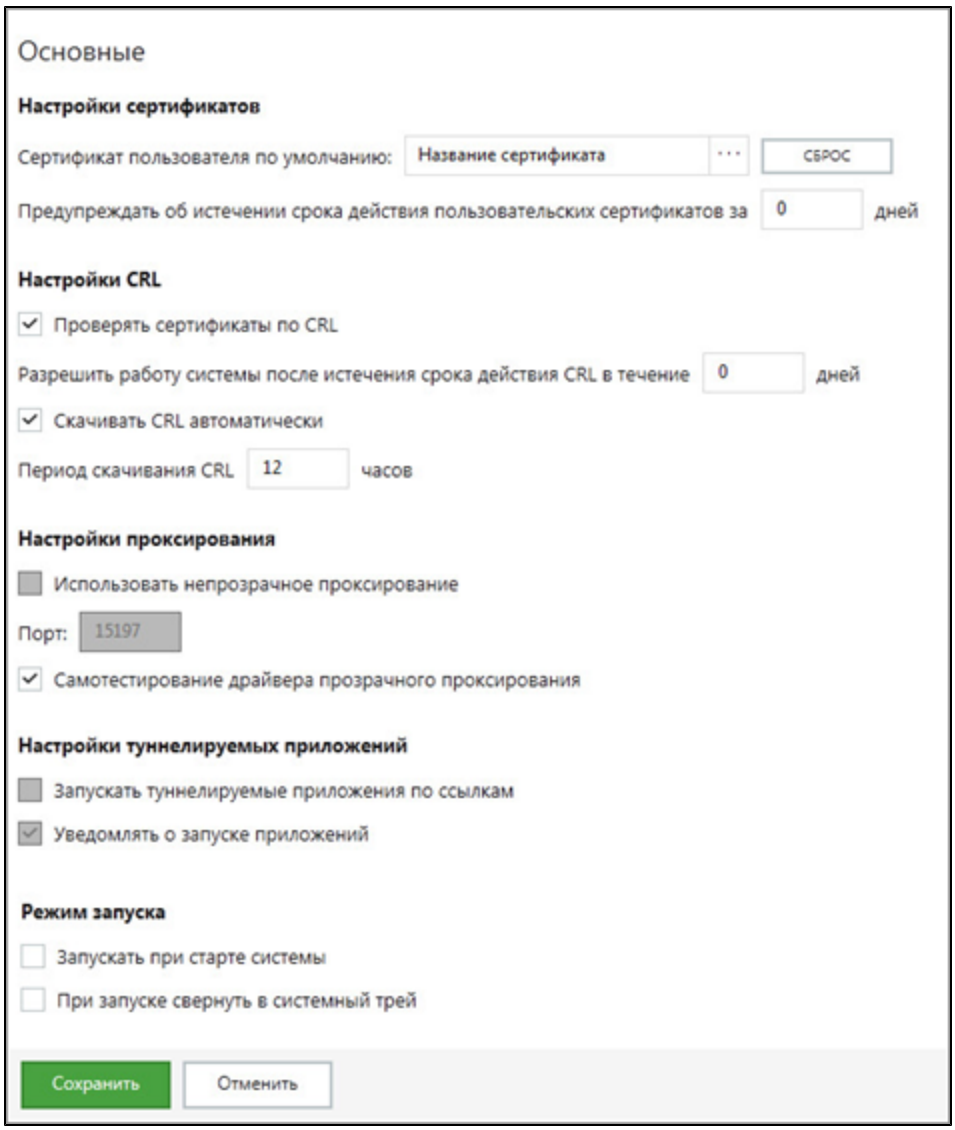


Основные настройки

Для настройки TLS-клиента:

1. Выберите в меню настроек пункт "Основные".

   В области отображения информации основного окна откроется соответствующее подменю.



2. Для автоматической аутентификации при подключении к TLS-серверу под определенным пользователем следует указать его сертификат, нажав кнопку …. В противном случае переходите к п. **4**.

Примечание. Если планируется подключение к ресурсам нескольких серверов, использовать данную настройку не рекомендуется.

На экране появится окно для выбора сертификата.

3. Укажите нужный сертификат и нажмите кнопку "ОК".

Примечание. Если сертификат пользователя, выбранный для подключения по умолчанию, станет недействительным, при попытке подключения появится сообщение о невозможности использования данного сертификата, а само подключение установлено не будет. Имя невалидного сертификата и его статус будет отображаться в разделе "Управление сертификатами", на вкладке "Пользовательские сертификаты". Для установки подключения выберите новый сертификат по умолчанию как описано выше.

4. Для организации проверки подлинности сертификата по CRL установите флажок "Проверять сертификаты по CRL".
5. Для настройки периода автоматического обновления сертификата CRL установите флажок "Скачивать CRL автоматически" и укажите нужный период в соответствующем поле.
6. В случае использования непрозрачного режима TLS-клиента установите отметку в поле "Использовать непрозрачное проксирование" и укажите выделяемый для этого порт (подробнее о настройках прокси см. стр.**30**).

7. Для включения самотестирования прозрачного режима проксирования при старте TLS- клиент поставьте соответствующую отметку (по умолчанию процедура отключена).
8. Для разрешения автоматического запуска туннелируемых приложений по гиперссылкам установите соответствующую отметку.
9. Настройте режим запуска ПО TLS-клиент при старте системы (по умолчанию включено).
10. Выберите режим отображения ПО после запуска (по умолчанию отображается значком в панели задач ОС Windows).
11. Для сохранения выполненных настроек нажмите кнопку "Сохранить".

Настройки прокси

Непрозрачное проксирование

Использование непрозрачного прокси- сервера дает возможность модифицировать запрос и/или ответы пользователя.
Если политики информационной безопасности вашей организации предусматривает непрозрачное проксирование, необходимо настроить параметры режима работы прокси-сервера.

Для использования непрозрачного копирования:

1. Запустите TLS- клиентот имени администратора и перейдите в раздел "Основные настройки".
2. Поставьте отметку в поле "Использовать непрозрачное проксирование"
3. Откроется окно настройки параметров прокси-сервера.
4. Укажите выделяемый для этого порт.

> **Внимание!** Порт непрозрачного режима — уникальный параметр, который необходимо вводить для каждого пользователя заново. При входе под учетной записью другого пользователя непрозрачный режим, несмотря на проставленную отметку, будет недоступен до тех пор, пока пользователь не укажет свой индивидуальный порт.

5. В настройках интернет-браузера укажите localhost в качестве адреса HTTP- и SSL-прокси-сервера, а также пропишите тот же порт.

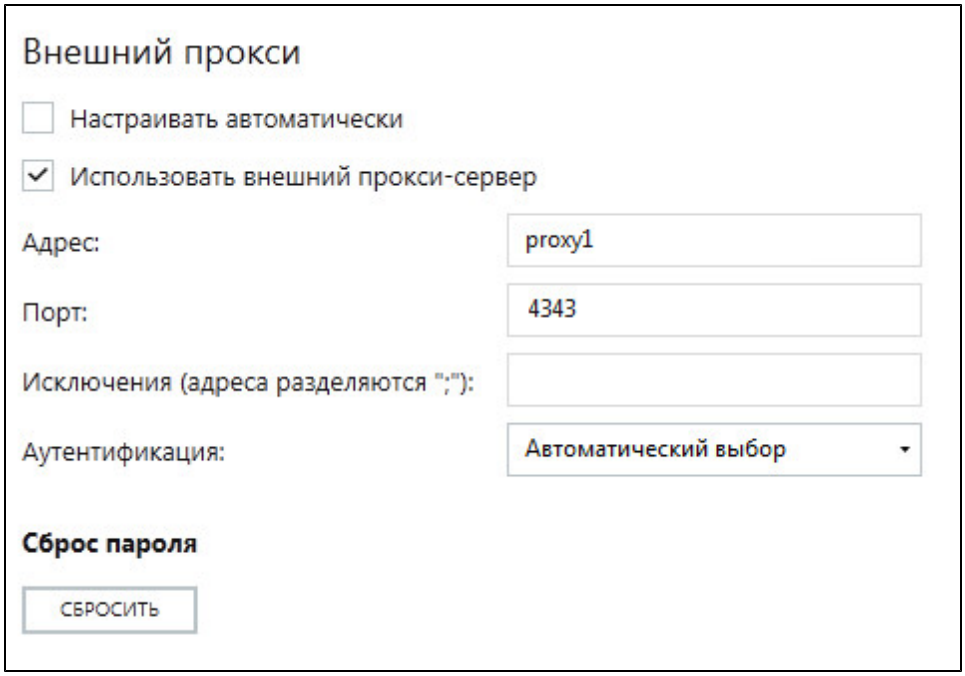
> **Примечание.** При использовании интернет-браузера Firefox для корректной работы в режиме непрозрачного проксирования необходимо импортировать корневой сертификат ContinentTLSClientRoot, находящийся в хранилище доверенных корневых центров сертификации, в хранилище сертификатов Firefox.

Внешний прокси

Для настройки подключения к интернет через внешний прокси-сервер вручную:

1. Выберите в меню настроек пункт "Внешний прокси".

   В области отображения информации основного окна отобразится соответствующий список настроек.

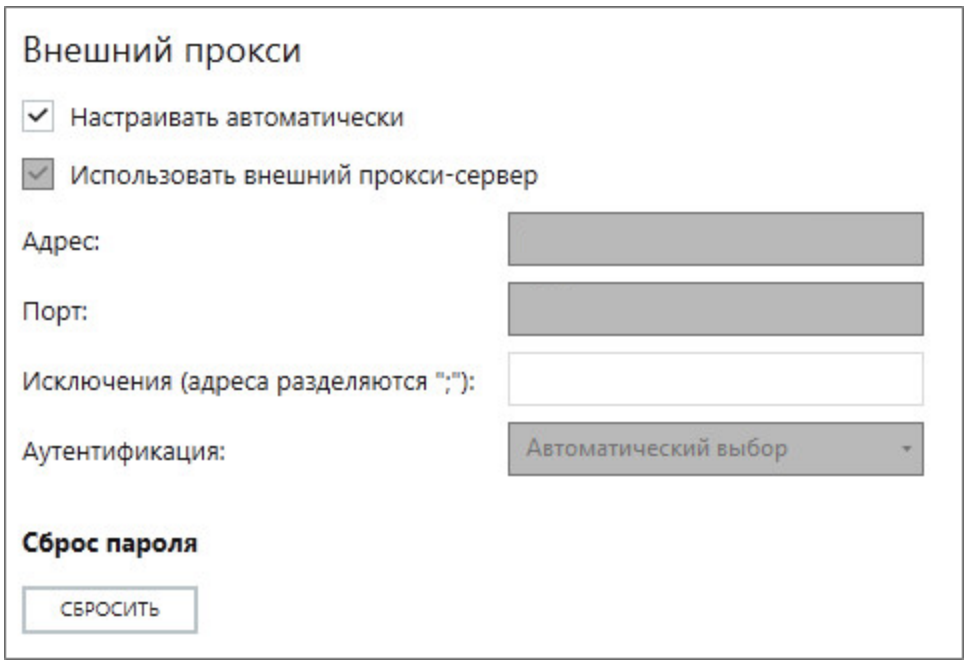


2. Установите отметку в поле "Использовать внешний прокси-сервер".
3. В поле "Адрес" введите IP-адрес или имя прокси-сервера. В поле "Порт" — порт для подключения к прокси-серверу.
4. Выберите способ аутентификации и заполните соответствующие данные.
5. При необходимости укажите список исключений (перечень IP-адресов или сетевых имен, разделенных символом ";").
6. Для завершения настройки и применения введенных или исправленных значений параметров нажмите кнопку "Сохранить".

Для автоматической настройки подключения к интернет через внешний прокси-сервер:

1. Выберите в меню настроек пункт "Внешний прокси".

   В области отображения информации основного окна отобразится соответствующий список настроек.



2. Установите отметку в поле "Настраивать автоматически".

3. TLS-клиент применит для настройки параметров прокси-сервера существующие настройки браузера автоматически.

Примечание. Список ресурсов будет автоматически помещен в исключения системных настройках браузера. В остальных полях графического интерфейса пользователя появятся значения, сохраненные в системных настройках.

4. Для применения настройки нажмите кнопку "Сохранить".

В настройках внешнего прокси-сервера предустмотрена возможность сброса текущего пароля для доступа к прокси-серверу.

Для сброса пароля к прокси-серверу:

1. Нажмите кнопку "Сбросить".
2. Нажмите кнопку "Да" в появившемся окне подтверждения.

При следующем подключении к удаленным ресурсам прокси-сервер потребует ввода нового пароля, который пользователь предварительно должен будет получить от администратора.

Управление конфигурацией

Настройками TLS-клиента предусмотрена возможность импорта / экспорта конфигурации настроек.

Для экспорта конфигурации TLS-клиента:

1. Перейдите в меню настроек в раздел "Управление конфигурацией" и выберите опцию "Экспортировать конфигурацию".

   Откроется окно проводника ОС Windows.
2. Укажите место хранения и название файла архива и нажмите кнопку "Сохранить".

   Появится сообщение об успешном завершении экспорта.
3. Нажмите кнопку "ОК", чтобы вернуться в раздел "Настройки.

Для импорта конфигурации TLS-клиента:

4. Перейдите в меню настроек в раздел "Управление конфигурацией" и выберите опцию "Импортировать конфигурацию".

   Откроется окно проводника ОС Windows.
5. Выберите нужный конфигурационный файл и нажмите кнопку "Открыть".

   Появится сообщение об успешном завершении импорта.
6. Нажмите кнопку "ОК", чтобы вернуться в раздел "Настройки.

Настройки обновления

Настройки обновления ПО

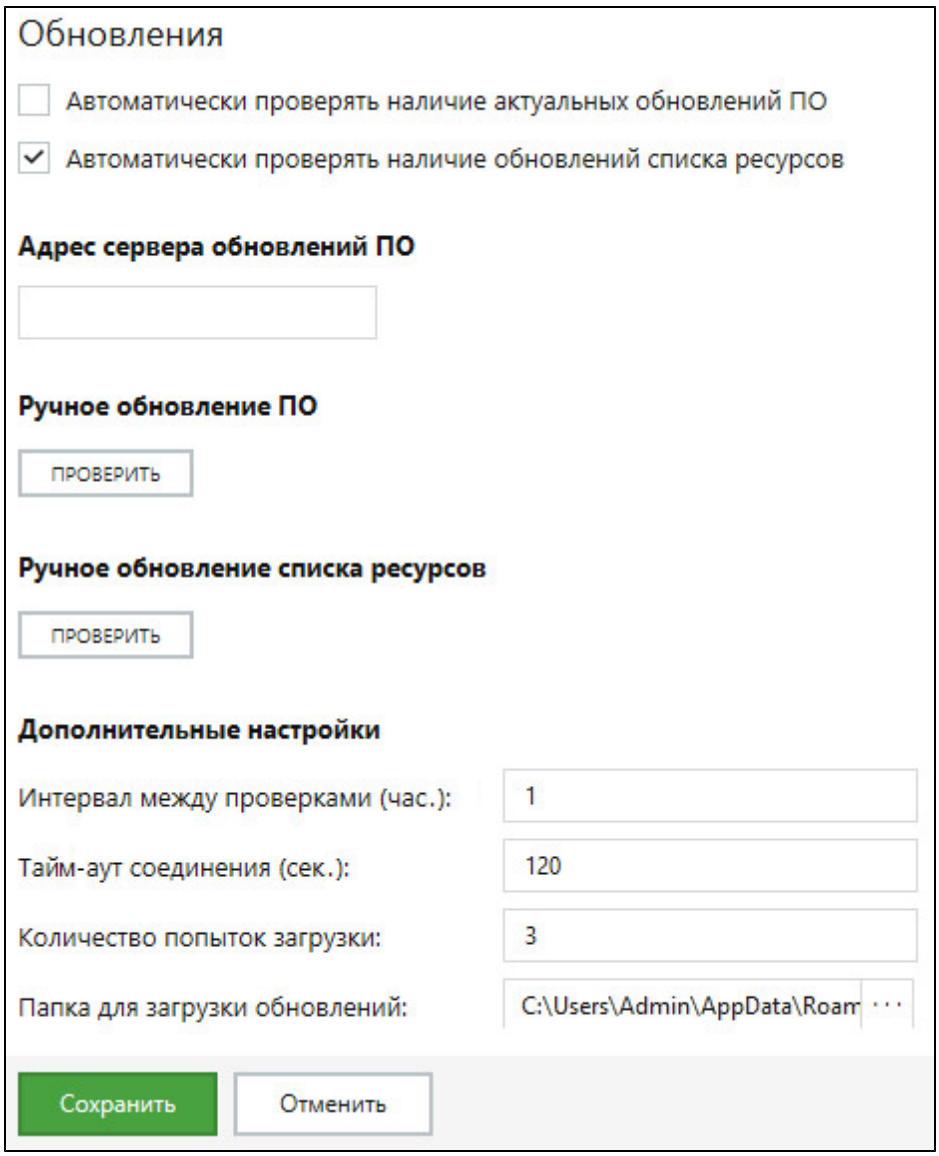
TLS-клиент позволяет автоматически проверять наличие обновлений ПО, хранящихся на TLS-сервере, а также скачивать и производить инсталляцию по запросу пользователя.

Внимание! Для управления настройками обновления и ручной проверки обновления требуется запустить TLS-клиент от имени администратора.

Для настройки обновления ПО:

1. Выберите в меню настроек TLS-клиента пункт "Обновления".

   Откроется список настроек:



2. Для настройки параметров обновления:
   - Введите имя сервера обновлений.

     Примечание. Наличие обновлений может проверить любой пользователь, для загрузки обновлений требуется аутентификация по сертификату, а для их установки — права локального администратора.
   - Для принудительной проверки наличия обновлений нажмите кнопку "Проверить".
   - При необходимости пропишите параметры автоматического обновления в подразделе дополнительных настроек.
3. Для завершения настройки нажмите кнопку "Сохранить".

Обновление списка ресурсов на TLS-серверах

TLS-клиент позволяет проверять наличие обновлений ресурсов сервера, с которым настроено соединение.

Для настройки обновления ресурсов сервера:

1. Выберите в меню настроек TLS-клиента пункт "Обновления".

   Откроется список настроек. Отметка в поле "Автоматически проверять наличие обновлений списка ресурсов" установлена по умолчанию.

Примечание Поиск наличия обновления проводится при каждом запуске графического интерфейса пользователя.
О порядке получения обновлений при автоматическом получении обновлений списка ресурсов сервера см . стр.27).

2. При необходимости провести принудительную проверку нажмите кнопку "Проверить" для ручного обновления списка ресурсов.

   Если обновления не были обнаружены, на экране появится соответствующее сообщение. При наличии обновлений появится сообщение о наличии обновлений конфигурации.

3. Нажмите на сообщение

   Внимание! Если необходимо отменить обновление, нажмите ✕.

   На экране появится окно выбора сертификата.

4. Выберите требуемый сертификат и нажмите кнопку "ОК".

   Внимание! Если в списке соединений указан один сервер, для которого будут выполняться проверки списка ресурсов, то в основных настройках можно выбрать сертификат пользователя по умолчанию. Если в списке соединений несколько серверов и для каждого необходим индивидуальный сертификат, применять данную опцию не рекомендуется. При наличии обновлений следует выбирать из списка индивидуальный сертификат для каждого сервера.

   На экране появится окно для ввода пароля для доступа к криптографическому контейнеру, если при создании контейнера не была выбрана опция "запомнить пароль".

5. Введите пароль и нажмите кнопку "ОК".

   После удачного обновления на экране появится сообщение о том, что список ресурсов сервера обновлен. Посмотреть его можно, выбрав нужный сервер в списке соединений.

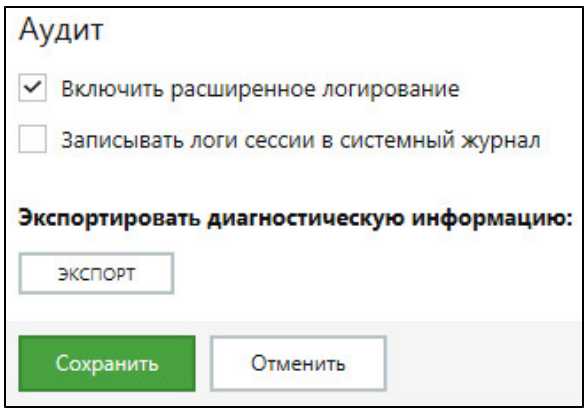
Настройка аудита

В системном журнале хранятся события узлов сети, служб TLS-клиента и другие системные события (см. стр.40).

Для настройки аудита:

1. Выберите в меню настроек TLS-клиента пункт "Аудит".

   В области отображения информации основного окна появится соответствующий список настроек.



2. Для включения расширенного логирования в настройках TLS-клиента установите отметку в соответствующем поле. Для отключения — снимите ее.

   Примечание. Лог-файлы содержат более полную информацию о событиях на узлах сети.

3. Для регистрации подключений к защищенным ресурсам в системном журнале установите отметку в соответствующем поле. Для отключения — снимите ее.

4. Для изменения настроек нажмите кнопку "Сохранить".

Для экспорта диагностической информации:

1. Выберите в меню настроек TLS-клиента пункт "Аудит".

   В области отображения информации основного окна появится соответствующий список настроек.

2. Для экспорта журналов аудита нажмите кнопку "Экспорт".

   На экране появится окно выбора ресурсов аудита.

3. Выберите нужную диагностическую информацию и нажмите кнопку "Экспорт".

   На экране появится окно проводника ОС Windows.

4. Укажите место хранения и название файла архива и нажмите кнопку "Сохранить".

   В случае успешного сохранения файла появится соответствующее сообщение.

   Внимание! В случае неоднократных сбоев работы ПО TLS-клиента файлы диагностической информации будут иметь большой размер, в результате чего процесс создания архива может занять длительное время. Для предотвращения переполнения жесткого диска в этом случае рекомендуется удалять дамп- файлы после решения проблемы (%PUBLIC%\ContinentTLSClient\ *.dmp).

5. Нажмите кнопку "ОК".

Внешний вид

Для настройки вида интерфейса TLS-клиента:

1. Выберите в меню настроек пункт "Внешний вид".

   В области отображения информации основного окна появится соответствующий список настроек.

2. Выберите тему оформления.

Эксплуатация TLS-клиента

Доступ к защищенным ресурсам

Для доступа к защищенному ресурсу:

Внимание! Если для доступа к защищенному ресурсу требуется аутентификация по сертификату, подключите внешний носитель с ключевой информацией.

1. Запустите веб- браузер (или консоль подключения к удаленному рабочему столу) и в адресной строке введите адрес защищенного ресурса.

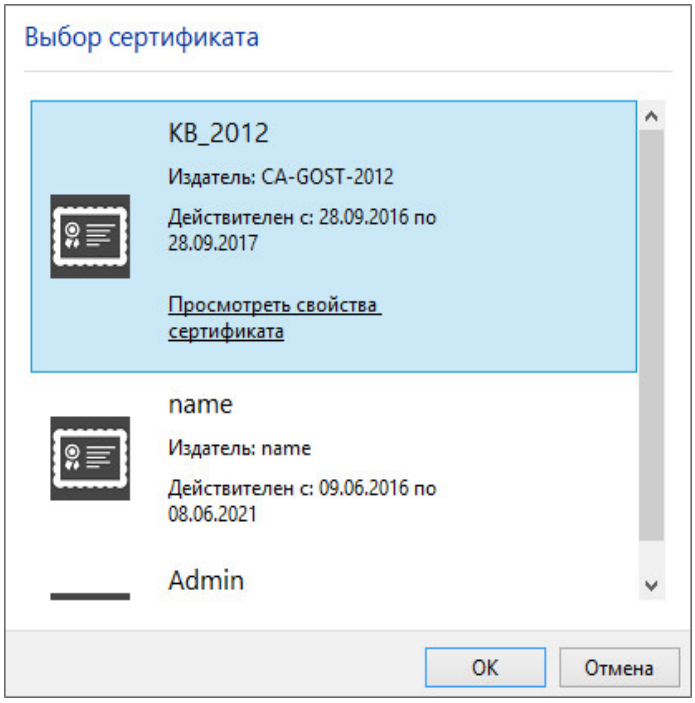
   Для подключений к защищённым ресурсам в веб-браузере рекомендуется использовать протокол HTTP, но допустимо так же использовать протокол HTTPS. Протокол указанный в браузере не влияет на защищённое соединение между TLS-клиентом и сервером.

   Внимание! При установленном туннеле необходимо в веб- обозревателе задавать тот же протокол, который используется на защищенном веб-сервере.

   Пример: https://172.20.20.7 или https://SRV или http://192.168.47.1:4444.

   Примечание. В случае использования сетевого имени ресурса вместо его адреса необходимо осуществить соответствующую настройку DNS-сервера или файла hosts. После внесения изменений в файл hosts необходимо перезапустить приложение TLS-клиента.

   Если не установлен сертификат по умолчанию (см. п. **2** процедуры настройки параметров TLS- клиента на стр.**29**), на экране появится окно выбора сертификата пользователя.



В диалоге отображается список установленных сертификатов.

2. Выберите сертификат пользователя и нажмите кнопку "OK".
3. Если на экране появится окно ввода пароля доступа к ключевому контейнеру — введите его и нажмите кнопку "OK".

Примечание. Если требуется запомнить пароль доступа, установите отметку в соответствующем поле.

Диалог выбора сертификата закроется, и будет установлено защищенное соединение с указанным ресурсом.

Если пользователь 5 раз подряд в течение 10 минут предъявил недействительный сертификат, то доступ к серверу заблокируется на 10 минут (ограничение реализовано на стороне сервера, его параметры настраиваемы).

Примечание. Если на TLS-сервере включен режим работы без аутентификации пользователя, то для доступа к защищенному ресурсу пользователю достаточно запустить веб-браузер и в адресной строке ввести адрес веб-ресурса.

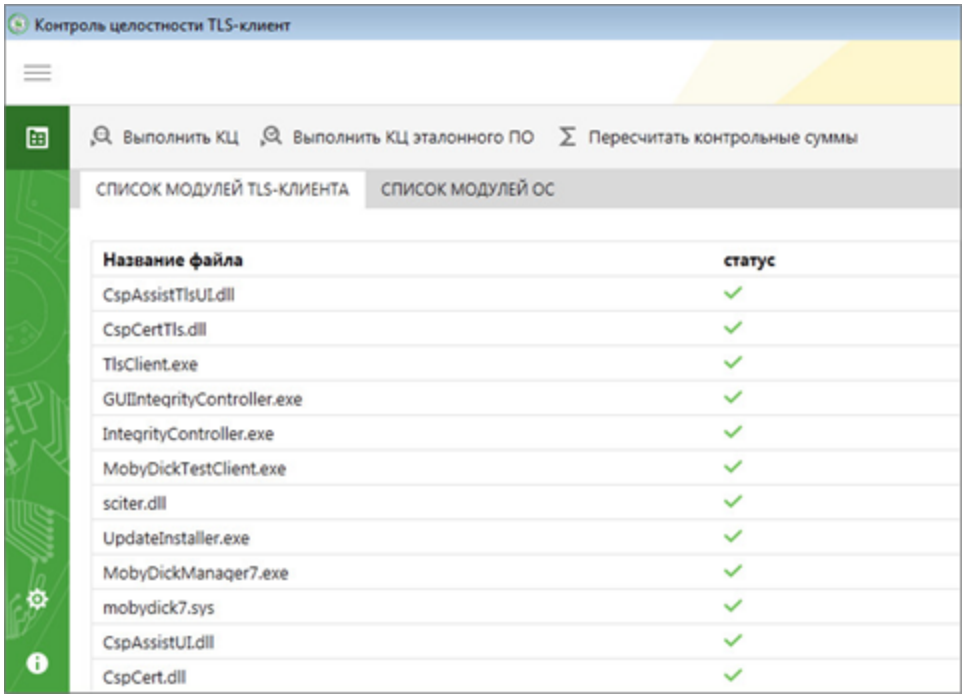
Контроль целостности

Для запуска УКЦ:

- Выберите в главном меню Windows пункт "Код Безопасности | Контроль целостности TLS-клиента".

Внимание! Для изменения настроек контроля целостности требуется запуск УКЦ от имени администратора.

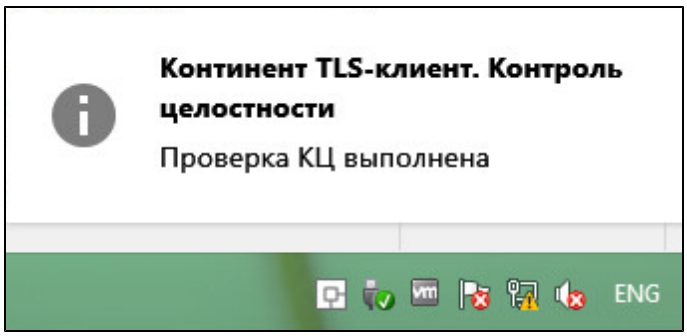
На экране появится основное окно утилиты.



Для выполнения контроля целостности системных файлов ПО TLS-клиента:

- В основном окне УКЦ выберите на панели инструментов пункт "Выполнить КЦ".

  Будет выполнена пофайловая процедура контроля целостности списка модулей TLS-клиента и ОС. В ходе ее выполнения проверенные файлы на экране будут отмечены знаком ✓. После успешного завершения процедуры на экране появится следующее информационное окно:



Для выполнения контроля целостности файлов дистрибутива ПО TLS-клиента:

1. В основном окне УКЦ выберите на панели инструментов команду "Выполнить КЦ эталонного ПО".

   На экране появится окно открытия каталога дистрибутива.

2. Укажите путь к файлам дистрибутива, нажав кнопку [...].

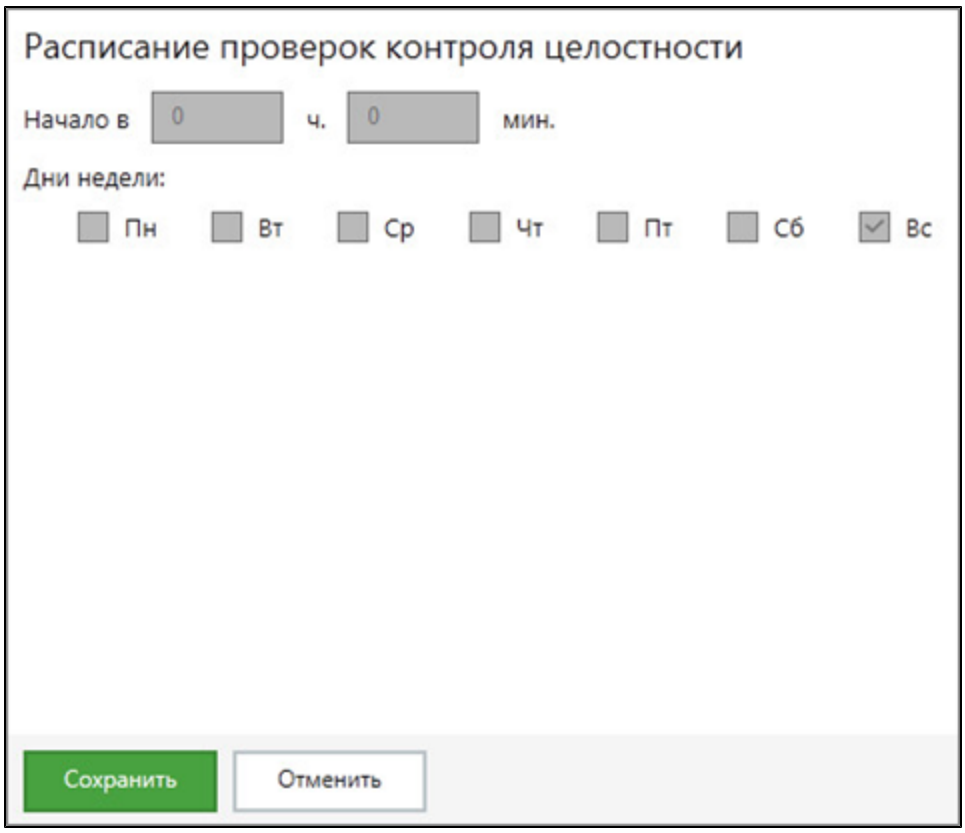
   Будет выполнена пофайловая процедура контроля целостности дистрибутива. После ее успешного завершения на экране появится соответствующее информационное окно.

Для настройки расписания регламентных проверок:

1. В основном окне УКЦ выберите в главном меню пункт вызова настроек.

   Внимание! Для изменения расписания регламентных проверок требуется запуск УКЦ от имени администратора.

   На экране появится текущее расписание регламентных проверок.



2. Укажите время и дни, в которые нужно проводить регламентные проверки.
3. Нажмите кнопку "Сохранить".

   Будет выполнено изменение настроек УКЦ, после чего на экране появится соответствующее информационное окно.
4. Нажмите кнопку "ОК".

Приложение

Требования к сертификатам

Устанавливаемые сертификат Сервера и сертификат пользователя должны иметь определенную структуру и отвечать ряду требований.

Структура и содержание сертификата Сервера

Для получения сертификата Сервера администратор должен сформировать запрос и отправить его в удостоверяющий центр. Параметры запрашиваемого сертификата предварительно настроены и подставляются автоматически при создании запроса.

Внимание! Проверкой актуальности сертификата Сервера занимается клиент.

В таблице ниже приведены общие характеристики свойств сертификата Сервера.

Табл.1 Структура и содержание сертификата Сервера

№ п/п	Параметр	Описание	Значение
Базовые поля сертификата			
1.1	Version	Версия	V3
1.2	Serial Number	Серийный номер	Уникальный серийный номер сертификата
1.3	Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.10-2001 или ГОСТ Р 34.10-2012
1.4	Issuer	Издатель сертификата, Поставщик	CN = Имя центра сертификации. O = Организация. C = Страна/Регион . E = Электронная почта
1.5	Valid from	Срок действия сертификата	Действителен с: дд.мм.гггг чч:мм:сс GMT
1.6	Valid to	Срок действия сертификата	Действителен по: дд.мм.гггг чч:мм:сс GMT
1.7	Subject	Владелец сертификата	CN = Имя сервера. OU = Подразделение. O = Организация. C = Страна/Регион (задается двумя латинскими буквами). E = Электронная почта
1.8	Public Key	Открытый ключ	Открытый ключ в соответствии с алгоритмом ГОСТ Р 34.10-2001 (512 Bits) или ГОСТ Р 34.10-2012 (512 Bits)
Дополнения сертификата			
2.1	Basic Constraints	Основные ограничения	Тип субъекта=Конечный субъект. Ограничение на длину пути=отсутствует
2.2	Key Usage	Использование ключа	Согласование ключа или цифровая подпись
2.3	Extended Key Usage	Улучшенный ключ	Проверка подлинности сервера (1.3.6.1.5.5.7.3.2)
2.4	CRL Distribution Point	Точка распространения списка отозванных сертификатов	URL=http://www.test.ru/test.crl

Структура и содержание сертификата пользователя

Валидность сертификата пользователя проверяется Сервером.
В таблице ниже приведены общие характеристики свойств сертификата пользователя.

Табл.2 Структура и содержание сертификата пользователя

№ п/п	Параметр	Описание	Значение
Базовые поля сертификата			
1.1	Version	Версия	V3
1.2	Serial Number	Серийный номер	Уникальный серийный номер сертификата
1.3	Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.10-2001 или ГОСТ Р 34.10-2012
1.4	Issuer	Издатель сертификата, Поставщик	CN = Имя центра сертификации. O = Организация. C = Страна/Регион. E = Электронная почта
1.5	Valid from	Срок действия сертификата	Действителен с: дд.мм.гггг чч:мм:сс GMT
1.6	Valid to	Срок действия сертификата	Действителен по: дд.мм.гггг чч:мм:сс GMT
1.7	Subject	Владелец сертификата	CN = ФИО. OU = Подразделение. O = Организация. C = Страна/Регион (задается двумя латинскими буквами). E = Электронная почта
1.8	Public Key	Открытый ключ	Открытый ключ в соответствии с алгоритмом ГОСТ Р 34.10-2001 (512 Bits) или ГОСТ Р 34.10-2012 (512 Bits)
Дополнения сертификата			
2.1	Basic Constraints	Основные ограничения	Тип субъекта=Конечный субъект. Ограничение на длину пути=отсутствует
2.2	Key Usage	Использование ключа	Согласование ключа или цифровая подпись, или зашифрование ключа
2.3	Extended Key Usage	Улучшенный ключ	Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)
2.4	CRL Distribution Point	Точка распространения списка отозванных сертификатов	URL=http://www.test.ru/test.crl

Список регистрируемых событий

Ниже приведен список событий, связанных с работой TLS- клиента и регистрируемых в журнале Windows. Для просмотра зарегистрированных событий пользователь должен входить в группу локальных администраторов компьютера.

Событие
Продукт: Континент TLS-клиент -- Установка завершена успешно

Продукт: Континент TLS-клиент -- Удаление завершено успешно
Осуществлен запуск TLS-клиента
TLS-клиент остановлен
Произошла системная ошибка:%сообщение%
*Установлено соединение с защищенным ресурсом: %имя ресурса%
*Разорвано соединение с защищенным ресурсом: %имя ресурса%
Защищенный сервер не прошел аутентификацию. Причина %причина%
Сервер отказал в аутентификации
Сервер разорвал соединение на этапе аутентификации
Инициализация процедуры проверки целостности файлов выполнена успешно. Количество контролируемых файлов: %число%
Ошибка инициализации процедуры проверки целостности файлов. Требуется переустановка Континент TLS-клиента
Проверка целостности файлов выполнена успешно
Нарушена целостность файлов. Создание новых сессий запрещено
Выполнен перерасчет контрольной суммы файла %имя_файла%
Сертификат сервера добавлен в хранилище. Кем выдан: %имя%. Кому выдан: %имя%. Серийный номер: %номер%
Сертификат сервера был удален. Кем выдан: %имя%. Кому выдан: %имя%. Серийный номер: %номер%
Добавление защищенного ресурса: %имя%
Удаление защищенного ресурса: %имя%
CRL импортирован в систему. Издатель: %имя%

Примечание. События с символом * регистрируются только при включенной опции "Записывать логи сессии в системный журнал" в настройках аудита.